

Syrian Arab Republic
Aleppo University
Faculty of Sciences
Math. Department

Nilpotent and Idempotent Elements in Some Rings

A Study Was Prepared for Master degree in Mathematics

Presented by:
Abd Al-Moean Jaddouh

الجمهورية العربية السورية
جامعة حلب
كلية العلوم
قسم الرياضيات



العناصر عديمة القوة والعناصر الجامدة في بعض الحلقات

دراسة أعدت لنيل شهادة الماجستير في الرياضيات

إعداد:
عبد المعين جدوع

٢٠٠٩ م – ١٤٣٠ هـ

الجمهورية العربية السورية
جامعة حلب
كلية العلوم
قسم الرياضيات



العناصر عديمة القوة والعناصر الجامدة في بعض الحلقات

دراسة أعدت لنيل شهادة الماجستير في الرياضيات

إعداد:

عبد المعين جدوع

إشراف:

الأستاذ الدكتور محمد خير أحمد **الدكتور نادر ضبيط**

أعضاء لجنة الحكم: التوقيع

- الأستاذ الدكتور محمد خير أحمد (مشرفاً) ....
- الأستاذ الدكتور نادر النادر ....
- الأستاذ الدكتور أحمد الغصين ....

نوقشت و أوصي بإجازتها بتاريخ ٢٠٠٩/٩/١٦ م

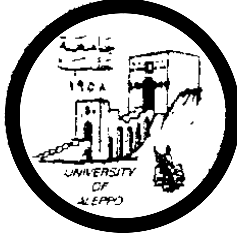
بسم الله الرحمن الرحيم

الجمهورية العربية السورية

جامعة حلب

كلية العلوم

قسم الرياضيات



العناصر عديمة القوة والعناصر الجامدة في بعض الحلقات

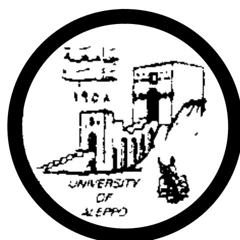
إعداد

عبد المعين جدوع

إشراف

أ.د. محمد خير أحمد   **د. نادر ضبيط**

الجمهورية العربية السورية
جامعة حلب
كلية العلوم
قسم الرياضيات



تصريح

أصرح بأن هذا البحث "العناصر عديمة القوة والعناصر الجامدة في بعض الحلقات" لم يسبق أن قبل للحصول على أي شهادة أخرى، كما أنه غير مقدم للحصول على أي شهادة أخرى.

المرشح
عبد المعين جدوع

Declaration

It's hereby declared that this work "Nilpotent and Idempotent Elements in Some Rings" hasn't already been accepted for any degree, nor it's being submitted for any other degree.

Candidate
Abd Al-moean Jaddouh

الجمهورية العربية السورية
جامعة حلب
كلية العلوم
قسم الرياضيات



شهادة

نشهد أن هذا العمل الموصوف في هذه الرسالة هو نتيجة بحث قام به المرشح طالب الدراسات العليا عبد المعين جدوع تحت إشراف الأستاذ الدكتور محمد خير أحمد و الدكتور نادر ضبيط في قسم الرياضيات، كلية العلوم، جامعة حلب، وأي رجوع إلى أي بحث آخر في هذا الموضوع موثق في النص.

المشرفان		المرشح
أ.د. محمد خير أحمد	**د. نادر ضبيط**	**عبد المعين جدوع**

Certification

It's certified that this work described in this thesis is the result of the author's own investigations under supervision of Prof. M.K. Ahmad and Dr. N. Dabbit in the department of mathematics, faculty of sciences, university of Aleppo, and any references to other researches work has been only acknowledged in the text.

Candidate	Dr.	Prof.
A.A. Jaddouh	**N. Dabbit**	**M.K. Ahmad**

شكر و تقدير

أتوجه بشكري وامتناني إلى أستاذي الدكتور محمد خير أحمد لتفضله بالإشراف على الرسالة، ولما قدمه من ملاحظات قيمة أغنت الرسالة.

حيث كان له الفضل الأكبر في تذليل كل الصعوبات والعقبات التي واجهتني أثناء إعداد الرسالة.

كما أتوجه بالشكر والتقدير للدكتور نادر ضبيط لمشاركته في الإشراف على الرسالة، والذي كان أحد أبحاثه نواة أولى لرسالتي هذه.

كما أتوجه بالشكر والتقدير إلى أعضاء لجنة المناقشة المحترمين لتفضلهم بمناقشة الرسالة.

وأخيراً لابد أن أشكر زملائي الأعزاء وكل من ساعدني في إعداد هذه الرسالة.

الإهداء

إلى بيلسان الروح و نبع الحنان الذي لاينضب، أمي ...

إلى رفيقة الدرب وشريكة العمر، زوجتي ...

إلى الأعزاء والأحباء، إخوتي ...

إلى كل من يؤمن بالعلم طريقاً للتقدم والإزدهار ...

الفهرس

العناصر عديمة القوة والعناصر الجامدة في بعض الحلقات

المقدمة:

تعتبر دراسة العناصر الخاصة، بشكل عام، (العناصر القاسمة للصفر Zero Divisor Elements – العناصر القابلة للقلب Invertible Elements – العناصر العديمة القوة Nilpotent Elements – العناصر الجامدة Idempotent Elements – العناصر النظامية Regular Elements) من المواضيع الهامة في نظرية الحلقات، لأنها تساعد بشكل كبير على إعطاء تصنيف للحلقات.

إن موضوع العناصر الجامدة والعناصر عديمة القوةفي الحلقات أخذ حيزاً كبيراً من الدراسات والبحوث الجبرية، القديمة منها و الحديثة، وذلك لأهمية هذا الموضوع.

لقد درس J. Krempa [13] العناصر الخاصة في حلقات أنصاف الزمر في بحثه (Special Elements in Semigroup Rings)، كما أفرد الرياضي J. Lambek [11] جزءاً كبيراً من كتابه الشهير (Lectures on Rings and Modules) لدراسة العناصر عديمة القوة في الحلقات، وجزءاً آخر لدراسة العناصر الجامدة في الحلقات، كذلك درس S. Sehgal [15] في كتابه (Topics In Group Rings) موضوع العناصر الجامدة والعناصر عديمة القوة في حلقات الزمر، كذلك خصص الباحث T. Y. Lam [10] جزءاً هاماً من كتابه (A First Course in Noncommutative Rings) لدراسة العناصر الجامدة في الحلقات غير التبديلية أيضاً درس نادر ضبيط [2]، في بحثه المنشور في العدد 43 من مجلة بحوث جامعة حلب لعام 2004 تحت عنوان (العناصر بقوة معدومة في الحلقات $\mathbf{Z}_n$)، موضوع العناصر عديمة القوة في الحلقات $\mathbf{Z}_n$، كما درس سامر عكور [3] العناصر الجامدة في حلقات الزمر في رسالة ماجستير نوقشت وأجيزت عام 2000 في جامعة آل البيت، كذلك درس أسامة علقم وعماد أبو إصبع [4] في بحثهما (On The Regular Elements in $\mathbf{Z}_n$) المنشور في 2007 العناصر النظامية في الحلقات $\mathbf{Z}_n$، كذلك درس StevenFinch [8] في بحثه (Idempotent and Nilpotent Modulo n) المنشور في 2006 العناصر الجامدة والعناصر عديمة القوة بالقياس n حيث حدد عددها في الحلقات $\mathbf{Z}_n$ ولكنه لم يحدد أشكالها.

كان هدفنا من هذه الرسالة البحث ايجاد طريقة يتم من خلالها تحديد العناصر الجامدة والعناصر عديمة القو ة في الحلقات $\mathbf{Z}_n$، وفي بعض الحلقات الأخرى.

تم تقسيم الرسالة إلى فصلين:

تضمن الفصل الأول، المعنون بأوليات عن الحلقات والعناصر الجامدة والعناصر عديمة القوة فيها، بندين اثنين، حيث نجد في البند الأول بعض المعلومات الأساسية عن الحلقات، بشكل عام، وعن الحلقات $\mathbf{Z}_n$، بشكل خاص، فيما تضمن البند الثاني بعض المعلومات الأساسية عن العناصر الجامدة و العناصر عديمة القوة.

أما الفصل الثاني، المعنون بالعناصر الجامدة والعناصر عديمة القوة في الحلقات $\mathbf{Z}_n$ وفي بعض الحلقات الأخرى، فقد تضمن ثلاثة بنود،تمكّنا في البند الأول من تحديد العناصر الجامدة، غير المبتذلة، في الحلقات $\mathbf{Z}_n$، و في البند الثاني تمكّنا من تحديد العناصر عديمة القوة، غير المبتذلة، في الحلقات $\mathbf{Z}_n$ و في البند الثالث حدّدنا العناصر الجامدة، غير المبتذلة، في الحلقات الإقليدية.

الفصل الأول

أوليات عن الحلقات و العناصر الجامدة والعناصر عديمة القوة فيها

سنقدم في هذا الفصل بعض المعلومات الأولية عن الحلقات بشكل عام و بشكل خاص عن الحلقات $\mathbf{Z}_n$، كما سنقدم بعض المعلومات عن العناصر الجامدة والعناصر عديمة القوة في الحلقات.

١.§ بعض الأوليات عن الحلقات:

تعريف (١-١-١):[10]

الحلقة: إذا كانت $R \neq \phi$ مجموعة ما، معرّف عليها عمليتين ثنائيتين داخليتين الأولى ترّمز بـ (+) و تسمى جمعاً، والثانية ترّمز بـ (.) وتسمى ضرباً، فإن $(R,+,.)$ تشكل حلقة إذا تحققت الشروط التالية:

(١) $(R,+)$ زمرة تبديلية.

(٢) عملية الضرب تجميعية على عناصر R، أي إن:

$$\forall x, y, z \in R \qquad ; \qquad x.(y.z) = (x.y).z$$

(٣) ترتبط العمليتان (+) و (.) فيما بينهما بقانوني التوزيع الآتيين:

$$\forall x, y, z \in R \qquad ; \qquad x.(y+z) = x.y + x.z$$
$$\forall x, y, z \in R \qquad ; \qquad (y+z).x = y.x + z.x$$

ملاحظات (١-١-٢):

(١) سنرمز فيما يأتي للحلقة بـ R عوضاً عن $(R,+,.)$.

(٢) تكون الحلقة R تبديلية إذا كانت العملية (.) عملية تبديلية على عناصر R، أي إذا تحقق الشرط التالي:

$$\forall x, y \in R \qquad ; \qquad x.y = y.x$$

(٣) العنصر الحيادي بالنسبة لعملية الجمع موجود دوماً، ويسمى بصفر الحلقة ويرمز له بالرمز 0.

(٤) نقول عن الحلقة R إنها ذات عنصر وحده (أو واحدية) (Unitary Ring) إذا احتوت على عنصر حيادي بالنسبة لعملية الضرب.

إذا كانت الحلقة R غير صفرية، فإن عنصر الوحدة فيها هو عنصر مختلف عن الصفر.

تعريف (١-١-٣):[17]

لتكن $(R,+,.)$ حلقة، ولتكن A مجموعة جزئية، غير خالية، من R. إذا كانت A حلقة تحت مقصوري العمليتين (+) و (.) على A، فإن A تسمى حلقة جزئية من الحلقة R.

ملاحظات (١-١-٤):[17]

- إذا كانت R حلقة، وكانت A حلقة جزئية منها، فإن:

١) ليس من الضروري أن تكون الحلقة الجزئية A ذات عنصر وحدة، حتى إن كانت الحلقة R ذات عنصر وحدة.

٢) ليس من الضروري أن تكون الحلقة R ذات عنصر وحدة، حتى إن كانت الحلقة الجزئية A ذات عنصر وحدة.

٣) ليس من الضروري أن يكون عنصر الوحدة للحلقة الجزئية A (إن وجد) هو نفسه عنصر الوحدة للحلقة R (إن وجد).

تعاريف (١-١-٤):

لتكن R حلقة ما عندئذٍ :

(١) العنصر القابل للقلب: إذا كانت الحلقة R تبديلية و ذات عنصر وحدة، فإننا نقول عن عنصر x من R إنه قابل للقلب (Unit)، إذا وجد عنصر $y \in R$، بحيث $x.y = y.x = 1$، ونرمز لـ y عادةً بالرمز x^{-1} ويسمى مقلوب x، و يرمز لمجموعة جميع العناصر القابلة للقلب في R بالرمز U_R.[17]

(كما ويمكن تعريف العنصر القابل للقلب من اليمين (من اليسار) في الحلقات غير التبديلية، ونقول عن العنصر القابل للقلب من اليمين ومن اليسار إنه عنصر قابل للقلب).[10]

(٢) العنصر القاسم للصفر: كانت الحلقة R تبديلية، فإننا نقول عن عنصر $a \in R$ إنه قاسم للصفر (Zero Divisor)، إذا وجد عنصر $b \neq 0$ من R بحيث يكون $a.b = 0$ (أو $b.a = 0$)، نجد هنا أن الصفر هو قاسم لنفسه، و يرمز لمجموعة جميع العناصر القاسمة للصفر في R بالرمز Z_R، ونقول عن عنصر $a \in R \setminus \{0\}$ إنه غير قاسم للصفر، إذا لم يكن بالإمكان إيجاد عنصر $b \neq 0$ من R بحيث $a.b = 0$ (أو $b.a = 0$).[17]

(كما ويمكن تعريف العنصر القاسم للصفر من اليمين (من اليسار) في الحلقات غير التبديلية، ونقول عن العنصر القاسم للصفر من اليمين ومن اليسار إنه عنصر قاسم للصفر).[10]

(٣) العنصر النظامي: نقول عن عنصر $a \in R$ إنه عنصر نظامي (Regular)، إذا وجد عنصر b من R بحيث يكون $a = aba$.[13]

(٤) العنصر الدوري: نقول عن عنصر $a \in R$ إنه عنصر دوري (Periodic)، إذا وجد عددان صحيحان موجبان ومختلفان n,m بحيث يكون $a^n = a^m$.[13]

تعاريف(١-١-٥):[10]

لتكن R حلقة عندئذٍ :

١) المثالية اليسارية: نقول عن مجموعة جزئية غير خالية I من الحلقة R إنها مثالية يسارية في الحلقة R إذا كانت تحقق الشرطين التاليين:

-١- إذا كان a,b عنصرين ما من I، فإن $a - b \in I$.

-٢- إذا كان r عنصراً ما من R، وكان a عنصراً ما من I، فإن $ra \in I$.

٢) المثالية اليمينية: نقول عن مجموعة جزئية غير خالية I من الحلقة R إنها مثالية يمينية في الحلقة R إذا كانت تحقق الشرطين التاليين:

-١- إذا كان a,b عنصرين ما من I، فإن $a - b \in I$.

-٢- إذا كان r عنصراً ما من R، وكان a عنصراً ما من I، فإن $ar \in I$.

٣) المثالية ثنائية الجانب: نقول عن مجموعة جزئية غير خالية I من الحلقة R إنها مثالية ثنائية الجانب في الحلقة R إذا كانت I مثالية يمينية ويسارية بآن واحد في الحلقة R.

تعاريف ونتائج (١-١-٦):[11]

لتكن R حلقة ما عندئذٍ :

-١- كل مثالية في الحلقة R هي حلقة جزئية منها، لكن ليس من الضروري أن تكون كل حلقة جزئية من الحلقة R مثالية في الحلقة R.

-٢- إذا كانت $R \neq \{0\}$، فإن الحلقة R تحوي مثاليتين، على الأقل، هما $R, \{0\}$, وكل مثالية في الحلقة R تختلف عن المثاليتين $R, \{0\}$ تسمى مثالية غير مبتذلة في الحلقة R.

-٣- إذا كانت R حلقة ذات عنصر وحدة، ورمزنا لعنصر وحدتها بالرمز 1، وكانت I مثالية ما في الحلقة R، ووجد في I عنصر له مقلوب في R بالنسبة للعملية (.), تكون عندها $R = I$.

تعاريف (١-١-٧):[17]

لتكن R حلقة ما،عندئذٍ :

١) المثالية الأولية: نسمي كل مثالية P في الحلقة R مثالية أولية فيها، إذا كانت $R \neq P$ و P تحقق الشرط:

- من أجل أي مثاليتين I, J من R بحيث $I.J \subseteq P$، فإنه إما أن يكون $I \subseteq P$ أو $J \subseteq P$.

٢) المثالية الأعظمية: نسمي كل مثالية M في الحلقة R مثالية أعظمية فيها، إذا كانت $R \neq M$ و لم يكن بالإمكان إيجاد مثالية I في الحلقة R تحوي M وبحيث تكون $I \neq R$ و $I \neq M$.

٣) المثالية الرئيسة: نسمي كل مثالية I في الحلقة R مثالية رئيسة، إذا كانت I مولدة بعنصر واحد من R وليكن، مثلاً، a وتكون عندها $I = aR = Ra$.

تعاريف (١-١-٨):[17]

لتكن Rحلقة, عندئذٍ :

(١) نقول عن R إنها بسيطة (Simple) إذا كانت تملك مثاليتين فقط هما $R, \{0\}$.

(٢) نقول عن R إنها نظامية (Regular) إذا كان جميع عناصرها نظامية.

(٣) نقول عن R إنها محلية (Local) إذا كانت تحوي مثالية أعظمية يمينية (يسارية) وحيدة.

(٤) نقول عن R إنها نيوثرية إلى اليمين (اليسار) (Right Noetherian) إذا كانت كل سلسلة صاعدة من مثاليات R اليمينية (اليسارية) من الشكل $I_1 \subseteq I_2 \subseteq I_3 \subseteq ...$ تتوقف عند عدد منته من الحدود، أي يوجد عدد صحيح موجب n بحيث يكون $I_n = I_{n+1} = I_{n+2} = ...$.

(٥) نقول عن R إنها أرتينية إلى اليمين (اليسار) (Right Artinian) إذا كانت كل سلسلة هابطة من مثاليات R اليمينية (اليسارية) من الشكل $I_1 \supseteq I_2 \supseteq I_3 \supseteq ...$ تتوقف عند عدد منته من الحدود، أي إنه يوجد عدد صحيح موجب n بحيث يكون $I_n = I_{n+1} = I_{n+2} = ...$.

تعاريف (١-١-٩):[11]

لتكن R حلقة عندئذٍ :

١) تقاطع جميع المثاليات الأعظمية اليمينية في الحلقة R يسمى جذر جاكبسون للحلقة R، ونرمز له بالرمز $RadR$.

٢) تقاطع جميع المثاليات الأولية في الحلقة R يسمى الجذر الأولي للحلقة R، ونرمز له بالرمز $radR$.

- إذا كانت الحلقة R واحدية، فإننا بوضوح نجد $radR \subseteq RadR$.

مبرهنة (١-١-١٠):[11]

لتكن R حلقة ذات عنصر وحدة عندئذٍ : الجذر $RadR$ يتكون من جميع العناصر r من R، والتي يكون من أجلها $1-rx$ قابلاً للقلب من اليمين في الحلقة R، لكل $x \in R$.

أي إن:

$$r \in RadR \iff R \text{ قابل للقلب في } 1 - rx \;\; ; \;\; \forall x \in R$$

تعريف وخواص (١-١-١١):[5]

لتكن R حلقة تبديلية عندئذٍ :

(١) إذا كان $a,b \in R \setminus \{0\}$ فإننا نقول إن b يقسم a في R، أو نقول إن b قاسم لـ a في R، أو نقول a يقبل القسمة على b في R، أو نقول إن a مضاعف لـ b في R، ونرمز لذلك بـ $b \mid a$، إذا كان بالإمكان إيجاد عنصر $c \in R$، على الأقل، بحيث يكون $a = b.c$. أما إذا كان b لا يقسم a في R، فإننا سنرمز لذلك بـ $b \nmid a$.

(٢) إذا كان $a,b,c \in R \setminus \{0\}$ بحيث $a \mid b$ و $b \mid c$، فإن: $a \mid c$.

(٣) إذا كان $a,b,c \in R \setminus \{0\}$ بحيث $a \mid b$ و $a \mid c$ فإن: $a \mid (\lambda b + \gamma c)$ وذلك $\forall \lambda, \gamma \in R$.

(٤) إذا كانت الحلقة R ذات عنصر وحدة، وكان $a \in R \setminus \{0\}$ قابلاً للقلب في R، فإن $a \mid r$ وذلك $\forall r \in R$.

تعريف (١-١-١٢):

ليكن a عدداً صحيحاً و nعدداً صحيحاً موجباً، عندئذٍ تنص خوارزمية القسمة على وجود عددين صحيحين وحيدين q,r بحيث $a = q.n + r \;\; ; \;\; 0 \le r < n$ حيث يسمى q ناتج قسمة a على n، بينما يسمى r باقي تلك القسمة، ونرمز لهذا الباقي بالرمز $\overline{a}$ وهو وحيد بنص خوارزمية القسمة وينتمي إلى $\mathbf{Z}_n = \{1,2,..,n-1\}$، والتي تسمى مجموعة بواقي القسمة على العدد الصحيح الموجب n.

لنزود المجموعة $\mathbf{Z}_n$ بعمليتي $\oplus,\otimes$ بالاعتماد على عمليتي الجمع والضرب العاديتين و باقي القسمة على n، كما يأتي:

$$a \oplus b = \overline{a+b} \;\; , \;\; a \otimes b = \overline{a.b} \;\; ; \;\; \forall a,b \in \mathbf{Z}_n$$

حيث $\overline{a+b}$ تعني الجمع العادي $a+b$ ثم أخذ باقي قسمة الناتج على n، بالمثل، فإن $\overline{a.b}$ يعني الضرب العادي $a.b$ ثم أخذ باقي قسمة الناتج على n.

إن كلاً من $\otimes,\oplus$ عملية ثنائية داخلية على المجموعة $\mathbf{Z}_n$، بسبب وحدانية باقي القسمة على العدد n، بالتالي $\mathbf{Z}_n$ حلقة تبديلية واحدية تحت عمليتي الجمع والضرب بالقياس n، وتسمى حلقة بواقي القسمة على العدد الصحيح الموجب n.

سنرمز اختصاراً فيما يأتي للعملية $\oplus$ بالرمز $(+)$ و للعملية $\otimes$ بالرمز $(.)$.

تعريف (١-١-١٣):[17]

لتكن R حلقة تبديلية ذات عنصر وحدة، نقول عن R إنها منطقة تكاملية إذا كانت R لا تحوي قواسم للصفر.

تعريف ونتائج (١-١-١٤):[17]

- لتكن R حلقة ذات عنصر وحدة، وليكن a,b عنصرين من R. نقول عن a,b نهما مترافقان إذا كان كلٌ منهما غير قاسم للصفر وكان $a \mid b$ و أيضاً $b \mid a$.

- لتكن R حلقة ذات عنصر وحدة، وليكن a,b,c عناصر من R بحيث $a = b.c$. إذا كان c قابلاً للقلب في R، فإن a,b مترافقين، لأنه: بما أن $a = b.c$، فإن $b \mid a$، وبما أن c قابلٌ للقلب في R، فإنه يوجد c^{-1} بحيث $b = a.c^{-1}$، وبالتالي $a \mid b$.

- لتكن R حلقة ذات عنصر وحدة، وليكن a عنصراً ما من R نسمي العناصر المرافقة لـ a والعناصر القابلة للقلب في R بالقواسم المبتذلة لـ a.

تعريف (١-١-١٥):[17]

لتكن R حلقة. نقول عن $a \in R \setminus \{0\}$ إنه عنصر غير قابل للتحليل، إذا كان a غير قابلٍ للقلب في R وكانت جميع قواسمه مبتذلة.

تعريف (١-١-١٦):[17]

لتكن R حلقة. نقول عن R إنها حلقة ذات تحليل وحيد، إذا تحقق الشرطان:

١) كل عنصر من R وغير قابل للقلب في R هو جداء عدد منته من عناصر R غير القابلة للتحليل.

٢) التحليل السابق وحيد باستثناء الترتيب والعناصر القابلة للقلب.

أمثلة عن الحلقات ذات التحليل الوحيد:

1) حلقة الأعداد الصحيحة.

٢) حلقات كثيرات الحدود بأي عدد من المتحولات وبمعاملات من أي حقل.

تعريف (١-١-١٧):[14]

الحلقة الإقليدية: إذا كانت R حلقة تبديلية ذات عنصر وحده، فإننا نقول عن R إنها حلقة إقليدية إذا كانت منطقة تكاملية، وفي مقابل كل عنصر a منها مختلف عن الصفر و ُضع عدد صحيح غير سالب $\psi(a)$، أي إن $\psi : R \setminus \{0\} \rightarrow \mathbf{Z}^{+} \cup \{0\}$، بحيث إن ψ يحقق الشرطين التاليين:

-١- إذا كان $a \neq 0$ و $b \neq 0$ عنصرين من R بحيث أن b يقسم a في R، فإن $\psi(b) \leq \psi(a)$.

-٢- من أجل كل عنصرين a و $b \neq 0$ من R يوجد عنصران q و r في R بحيث يكون:

$$a = b.q + r$$

و r إما أن يكونصفراً أو يكون $\psi(r) < \psi(b)$.

ملاحظة (١-١-١٨):[14], [17]

بعض المراجع تشترط على الحلقة الإقليدية أن تكون منطقة تكاملية، و بعض المراجع لا تشترط ذلك، فعلى سبيل المثال نجد Samuel لم يشترط على الحلقة الإقليدية أن تكون منطقة تكاملية، فهو برهن على أنه إذا كانت $A_1, A_2, ..., A_m$ حلقات إقليدية، فإن $A_1 \times A_2 \times ... \times A_m$ هي أيضاً حلقة إقليدية، رغم أنها قد لا تكون منطقة تكاملية.

تعريف (١-١-١٩):[17]

إذا كانت R حلقة، فإننا نقول عن العنصر p من R، غير القابل للقلب في R، إنه عنصر أولي، إذا تحقق ما يأتي:

أي جداء لعنصرين من R يقبل القسمة على p فقط، وفقط إذا، كان أحد العنصرين، على الأقل، يقبل القسمة على p ، أي إذا قسم p جداء أي عنصرين من الحلقة R ، فإنه يقسم أحدهما، على الأقل.

نتيجة (١-١-٢٠):[17]

في الحلقات الإقليدية كل عنصر غير قابل للتحليل هو عنصر أولي، وبالعكس كل عنصر أولي هو عنصر غير قابل للتحليل.

مبرهنة (١-١-٢١):[17]

كل حلقة إقليدية هي حلقة ذات تحليل وحيد.

ملاحظة (١-١-٢٢): [14]

لتكن الحلقة $\mathbf{Z}_p$ بحيث p عدداً أولياً ، عندئذ $\mathbf{Z}_p$ حقل، وعليه فإن $\mathbf{Z}_p$ تكون حلقة إقليدية.

بالتالي إذا كان p,q عددين أوليين مختلفين، فإنه بالاعتماد على أن $\mathbf{Z}_p \times \mathbf{Z}_q \approx \mathbf{Z}_{p\times q}$، وبالاستفادة من الملاحظة (١-١-١٨)، تكون $\mathbf{Z}_{p\times q}$، أيضاً ، حلقة إقليدية بالرغم من وجود قواسم للصفر فيها.

مبرهنة (١-١-٢٣): (المبرهنة الأساسية في الحساب)[5]

كل عدد صحيح $1<n$ يكتب بشكل وحيد، باستثناء الترتيب، كحاصل ضرب عدد منته من الأعداد الأولية.

نتائج (١-١-٢٤):[9]

١) إذا كان a,b عددين صحيحين بحيث $\gcd(a,b)=1$، قلنا إنهما أوليان نسبياً .

٢) ليكن n ، m عددين صحيحين أولين نسبياً . إذا كان d قاسماً موجباً للعدد $n.m$ (أي $d>0$ و $d\,|\,n.m$)، فإنه يوجد عددان صحيحان موجبان d_1,d_2 بحيث $d=d_1.d_2\ \&\ (d_1,d_2)=1$ ويكون $d_1\,|\,n,\ \ d_2\,|\,m$.

٣) إذا كان a,b عددين صحيحين أولين نسبياً ، وكان $a.b=c^n$ ، فإنه يوجد عددان صحيحان e,d بحيث $a=d^n$ و $b=e^n$.

تعريف (١-١-٢٥): [6],[16],[12]

ليكن n عدداً صحيحاً موجباً بحيث $1 < n$، إن إمكانية كتابة n كحاصل ضرب عدد منته من الأعداد الأولية، تسمى تحليل n إلى عوامله الأولية، والشكل القياسي لهذا التحليل هو: $n = p_1^{m_1}.p_2^{m_2}....p_k^{m_k}$، حيث $p_1, p_2,.., p_k$ هي العوامل الأولية المختلفة للعدد n، وحيث $1 \le m_i$ يمثل عدد مرات تكرار العامل p_i لكل $i \in \{1,2,..,k\}$.

- في الحالة الخاصة عندما يكون العدد الصحيح $n = p$ أولياً، فإن $k = 1$ و $m_1 = 1$ أي إن $n = p_1$.

- في الحالة الخاصة عندما يكون العدد الصحيح n غير أولي ويكون $m_1 = m_2 = .. = m_k = 1$، أي عندما تكون العوامل الأولية لـ n مختلفة مثنى مثنى وغير مكررة، فإن العدد n يكتب بالشكل $n = p_1.p_2....p_k$ حيث $k \ge 2$، في هذه الحالة نسمي العدد غير الأولي n بسيطاً.

مبرهنة (١-١-٢٦): [9]

لتكن $a_1, a_2,.., a_n$ أعداداً صحيحة وليكن p عدداً أولياً بحيث $p \mid a_1.a_2....a_n$، عندئذٍ p يقسم واحداً، على الأقل، من الأعداد الصحيحة $a_1, a_2,.., a_n$.

نتيجة (١-١-٢٧): [9]

ينتج عن المبرهنة السابقة عندما نضع $a = a_1 = a_2 = .. = a_n$ أنه إذا كان $p \mid a^n$، فإن $p \mid a$ لكل عدد صحيح موجب n.

مبرهنة (١-١-٢٨): [6]

ليكن a,b عددين صحيحين ليس كلاهما صفراً، عند ذلك يتحقق $\gcd(a,b) = 1$ إذا، وفقط إذا، وجد عددان صحيحان x, y بحيث $ax + by = 1$.

تعريف (١-١-٢٩): [6]

ليكن n عدداً صحيحاً موجباً و ليكن a,b عددين صحيحين. نقول إن العدد الصحيح a يطابق العدد الصحيح b بالقياس n إذا، وفقط إذا، كان n يقسم الفرق $a - b$، أو بكلمة أخرى $a - b$ مضاعف لـ n، و نرمز لذلك بالرمز $a \equiv b \pmod n$.

أي إن:

$$a \equiv b \pmod{n} \Leftrightarrow n \mid a-b$$

ينتج، من التعريف السابق مباشرة، أنه إذا كان $a=\beta.n+\alpha$، حيث $a,\alpha,\beta \in \mathbf{Z}$ و $n \in \mathbf{Z}^{+}$، (أي إذا كان α هو باقي قسمة a على n)، فإن $a \equiv \alpha \pmod{n}$.

سنرمز لباقي قسمة a على n بالرمز $\overline{a}^{n}$ أو بالرمز $\overline{a}$ إذا لم يؤدِّ هذا الرمز إلى وقوع لبس.

ملاحظة (١-١-٣٠):[16]

ليكن $a \in \mathbf{Z}$ ولتكن الحلقة $\mathbf{Z}_n$ عندئذٍ وفقاً لما وجدنا سابقاً يكون $\overline{a} \in \mathbf{Z}_n$، فإذا كان $a<n$، فإن $a=\overline{a} \in \mathbf{Z}_n$، مع العلم أن a هنا يمثل صفاً من العناصر ولا يمثل نفسه فقط.

مبرهنة (١-١-٣١):[9]

ليكن a,b عددين صحيحين، وليكن باقي قسمتهما على العدد الصحيح الموجب n هو $\overline{a},\overline{b}$ على الترتيب،عندئذٍ :

$$\overline{a}=\overline{b} \Leftrightarrow a \equiv b \pmod{n}.$$

مبرهنة (١-١-٣٢):[16]

ليكن n عدداً صحيحاً موجباً ولتكن a,b,c,d أعداد صحيحة بحيث:

$$a \equiv b \pmod{n} \quad \& \quad c \equiv d \pmod{n}$$

عند ذلك يصح ما يأتي:

$$a+c \equiv (b+d) \pmod{n}$$

$$a-c \equiv (b-d) \pmod{n}$$

$$a.c \equiv b.d \pmod{n}$$

$$a.e \equiv b.e \pmod{n} \quad ; \quad \forall e \in \mathbf{Z}$$

مبرهنة (١-١-٣٣):[12]

ليكن nعدداً صحيحاً موجباً ، ولتكن a,b,c أعداداً صحيحة بحيث $c \neq 0$ عندئذٍ :

$$a.c \equiv b.c(\text{mod}\, n) \Leftrightarrow a \equiv b(\text{mod}\, \frac{n}{\gcd(c,n)})$$

- في الحالة الخاصة إذا كان $\gcd(c,n)=1$ ، فإن:

$$a.c \equiv b.c(\text{mod}\, n) \Leftrightarrow a \equiv b(\text{mod}\, n)$$

- وفي الحالة الخاصة إذا كان $n=p$ عدداً أولياً ، ولم يكن c مضاعفاً لـ p ، (أي $\gcd(p,c)=1$)، فإن:

$$a.c \equiv b.c(\text{mod}\, p) \Leftrightarrow a \equiv b(\text{mod}\, p)$$

مبرهنة (١-١-٣٤):[9]

إذا كان n,m عددين صحيحين موجبين، وكان a,b عددين صحيحين بحيث $a \equiv b(\text{mod}\, n)$ و $a \equiv b(\text{mod}\, m)$ ، فإن:

$$a \equiv b(\text{mod}[m,n])$$

حيث يشير الرمز $[n,m]$ إلى المضاعف المشترك الأصغر للعددين n,m.

وفي الحالة الخاصة عندما $\gcd(n,m)=1$ ، يكون $a \equiv b(\text{mod}\, m.n)$.

مبرهنة (١-١-٣٥):[9]

إذا كان n,m عددين صحيحين موجبين بحيث $m \mid n$ ، وكان a,b عددين صحيحين بحيث $a \equiv b(\text{mod}\, n)$ ، فإن $a \equiv b(\text{mod}\, m)$ ، أي إن:

$$a \equiv b(\text{mod}\, n)\ \&\ m \mid n \Rightarrow a \equiv b(\text{mod}\, m)$$

تعريف (١-١-٣٦):[9]

ليكن nعدداً صحيحاً موجباً وليكن $a \in \mathbf{Z}$. نقول عن $b \in \mathbf{Z}$ إنه نظير ضربي لـ a بالقياس n إذا، وفقط إذا، كان $a.b \equiv 1(\text{mod}\, n)$.

- ليس من الضروري أن يكون لكل عدد صحيح نظير ضربي.

مبرهنة (١-١-٣٧):[9]

إذا كان n عدداً صحيحاً موجباً، وكان $a \in \mathbf{Z}$، فإنه يوجد نظير ضربي للعدد a بالقياس n إذا، وفقط إذا، كان $\gcd(a,n)=1$.

مبرهنة (١-١-٣٨):[9]

ليكن $a,b \in \mathbf{Z}$ بحيث $i \in \{1,2,..,k\}$; $a \equiv b(\bmod n_i)$، وذلك أياً كانت الأعداد الصحيحة الموجبة $n_1, n_2,.., n_k$، فإن $a \equiv b(\bmod [n_1, n_2,..., n_k])$.

- في الحالة الخاصة، إذا كانت الأعداد الصحيحة $n_1, n_2,.., n_k$ أولية نسبياً مثنى مثنى، (أي $\gcd(n_i, n_j)=1$ لكل $1 \le i \ne j \le k$)، فإنه يتحقق $a \equiv b(\bmod n_1.n_2....n_k)$.

تعريف (١-١-٣٩):[9]

دالة أولر هي التطبيق $\varphi : \mathbf{Z}^+ \to \Re$، حيث $\varphi(n)$ يمثل عدد الأعداد الأولية نسبياً مع n، والتي هي أصغر من n وأكبر أو تساوي الصفر و ذلك من أجل كل n من $\mathbf{Z}^+$، أي إن:

$$\begin{aligned} \varphi(n) &= \left|\{x \in \mathbf{Z}; \gcd(x,n)=1 \,\&\, 0 \le x < n\}\right| \quad ; \quad \forall n \in \mathbf{Z}^+ \\ &= \left|\{x \in \mathbf{Z}_n; \gcd(x,n)=1\}\right| \quad ; \quad \forall n \in \mathbf{Z}^+ \end{aligned}$$

- في الحالة الخاصة، إذا كان $n=p$ عدداً أولياً ، فإن $\varphi(n)=\varphi(p)=p-1$.

مبرهنة أولر (١-١-٤٠):[9]

إذا كان n عدداً صحيحاً موجباً، وكان $a \in \mathbf{Z}$ بحيث $(a,n)=1$، فإنه يتحقق:

$$a^{\varphi(n)} \equiv 1(\bmod n)$$

حيث $\varphi(n)$ هي دالة أولر.

- في الحالة الخاصة، إذا كان $n=p$ عدداً أولياً ، بحيث $p \nmid a$ (أي $\gcd(a,p)=1$)، فإن $a^{p-1} \equiv 1(\bmod n)$. (مبرهنة فيرما).

٢.§ العناصر الجامدة والعناصر عديمة القوة في الحلقات وخواصها:

سنتعرف، في هذا البند، على نوعين هامين من العناصر الخاصة في الحلقات، وهما العناصر الجامدة، غير المبتذلة، و العناصر عديمة القوة، غير المبتذلة، كما سنقدم بعضاً من خواصها في الحلقات.

تعاريف (١-٢-١): [1]

لتكن R حلقة عندئذٍ :

١) نقول عن عنصر $x \in R$ إنه عديم القوة (Nilpotent) إذا وجد عدد صحيح موجب n بحيث $x^n = 0$، ويرمز لمجموعة جميع العناصر عديمة القوة في R بالرمز N_R، أي إن:

$$N_R = \{x \in R \ : \ \exists n \in \mathbf{Z}^+ \ ; \ x^n = 0\}$$

٢) نقول عن عنصر $x \in R$ إنه عديم القوة بسيط (Simple Nilpotent) إذا كان $x^2 = 0$، ويرمز لمجموعة جميع العناصر عديمة القوة البسيطة في R بالرمز SN_R، أي إن:

$$SN_R = \{x \in R \ ; \ x^2 = 0\}$$

٣) نقول عن عنصر عديم القوة $x \in R$، إنه عديم القوة مبتذل (Trivial)، إذا كان $x = 0$، حيث 0 هو صفر الحلقة R.

٤) نقول عن مثالية يمينية (يسارية، مثالية) I في الحلقة R، إنها عديمة القوة، إذا وجد عدد صحيح موجب n بحيث يكون $I^n = \{0\}$، وهذا يعني أن $a_1.a_2....a_n = 0$ لأي مجموعة عناصر $a_1, a_2, ..., a_n$ من I، ومنه $a^n = 0$ لكل a من I.

٥) نقول عن مثالية يمينية (يسارية، مثالية) I في الحلقة R، إنها منعدمة (Nil)، إذا كانت جميع عناصرها عديمة القوة.

نتائج (١-٢-٢): [1]

-١- كل عنصر عديم القوة بسيط هو عنصر عديم القوة، أي إن $\{0\} \subseteq SN_R \subseteq N_R$.

-٢- لتكن R حلقة ذات عنصر وحدة، وليكن $x \in R$ عنصراً عديم القوة، عندئذٍ يكون $(1-x)$ عنصراً قابلاً للقلب في R.

-٣- كل عنصر عديم القوة هو عنصر قاسم للصفر.

-٤- إذا كانت R حلقة تبديلية، فإن مجموعة جميع العناصر عديمة القوة N_R ، تشكل مثالية في الحلقة R .

-٥- إذا كانت R حلقة تبديلية، فإن مجموعة جميع العناصر عديمة القوة N_R ، تساوي تقاطع جميع المثاليات الأولية في الحلقة R .

مبرهنة (١-٢-٣): [11]

لتكن R حلقة تبديلية ذات عنصر وحدة عندئذٍ يتكون $radR$ -الجذر الأولي لـ R- (انظر(١-١-٩)) من جميع العناصر عديمة القوة في R .

البرهان:

ليكن r عنصراً عديم القوة في R، عندئذٍ :

$$\exists n \in \mathrm{N} \quad ; \quad r^n = 0$$

وبالتالي من أجل أي مثالية أولية P في الحلقة R يكون $r^n = o \in P$ ، وبالتالي $r \in P$ وعليه $r \in rad \quad R$.

العكس: ليكن r عنصراً ليس عديم القوة، عندئذٍ المجموعة $T = \{1, \mathrm{r}, \mathrm{r}^2, \ldots\}$ لا تحوي الصفر.

الآن، لتكن P عنصراً أعظمياً في مجموعة كل المثاليات، في R ، غير المتقاطعة مع T.

إن P مثالية أولية، لأنه: إذا كان $a,b \in R$ بحيث $a,b \in P$، فإن أحد العنصرين a,b، على الأقل، ينتمي إلى P ، وذلك لأنه:

إذا كان $a \notin P \,\&\, b \notin P$، فإن $P + aR$ ، $P + bR$ تتقاطع مع T، وبالتالي يوجد في T عنصران r^n ، r^m بحيث يكون:

$$r^m \in P + aR \quad \& \quad r^n \in P + bR \Rightarrow$$
$$r^{m+n} = r^m . r^n \in P \bigcap T$$

وهذا مناقض لكون P لا تتقاطع مع T.

وبما أن $r \notin P$ ، فإن r لا تنتمي إلى الجذر الأولي لـ R .

ملاحظة (١-٢-٤): [11]

إذا كانت الحلقة R شبه أولية (semi prime)، أي $radR=\{0\}$، فإن هذا يعني أن R لا تملك أية عناصر عديمة القوة غير مبتذلة.

تعاريف (١-٢-٥):

لتكن R حلقة، عندئذٍ :

١) نقول عن عنصر $x\in R$ إنه جامد (Idempotent)، إذا كان $x^2=x$، ويرمز لمجموعة جميع العناصر الجامدة في R بالرمز I_R، أي إن: $I_R=\{x\in R \;\; ; \;\; x^2=x\}$.[1]

٢) نقول عن عنصر $x\in R$ إنه جامد مبتذل، إذا كان $x=0$ (أو $x=1$ إذا كانت الحلقة R واحدية). [1]

٣) نقول عن عنصرين جامدين e,f إنهما متعامدان (Orthogonal) إذا كان $e.f=f.e=0$.[1]

٤) نقول عن عنصر جامد e إنه عنصر جامد ابتدائي (Primitive)، إذا لم نستطع كتابة e بالشكل $e=e_1+e_2$ ، حيث e_1 و e_2 جامدان متعامدان مختلفان عن الصفر. [1]

٥) نقول عن عنصر جامد e من R إنه مركزي (Central)، إذا كان $er=re$ وذلك لكل r من R ، (أي إن العنصر الجامد المركزي هو العنصر الجامد الذي يتبادل مع جميع عناصر الحلقة). [7]

٦) إذا كان e عنصراً جامداً من R ، فإن $f=1-e$، يكون، أيضاً، عنصراً جامداً يعامد e، لأن: $f^2=(1-e)(1-e)=1-e-e+e=1-e$.

وكذلك فإن $e.f=f.e=0$ ، إذن $f=1-e$ يعامد e .

أمثلة (١-٢-٦):

-١- في حلقة المصفوفات المربعة من المرتبة الثالثة فوق حقل الأعداد الحقيقية $\Re$ ، $M_{3\times3}(\Re)$ ، لدينا $a=\begin{pmatrix}0&1&0\\0&0&1\\0&0&0\end{pmatrix}$ عنصر عديم القوة غير مبتذل لأن $a^3=0$.

٢- في حلقة المصفوفات المربعة من المرتبة الثالثة فوق حقل الأعداد الحقيقية $\Re$، $M_{3\times3}(\Re)$، لدينا $b=\begin{pmatrix}0&1&0\\0&0&0\\0&0&0\end{pmatrix}$ عنصر عديم القوة بسيط لأن $b^2=0$.

٣- في حلقة المصفوفات المربعة من المرتبة الثانية فوق حقل الأعداد الحقيقية $\Re$، $M_{2\times2}(\Re)$، لدينا $e=\begin{pmatrix}1/2&1/2\\1/2&1/2\end{pmatrix}$ عنصر جامد غير مبتذل لأن $e^2=e$.

٤- في الحلقة $\mathbf{Z}_{27}$ لدينا $a=3$ عنصر عديم القوة غير مبتذل، لأن $a^3=3^3\equiv 0(\text{mod } 27)$.

٥- في الحلقة $\mathbf{Z}_9$ لدينا $b=3$ عنصر عديم القوة بسيط، لأن $b^2=3^2\equiv 0(\text{mod } 9)$.

٦- في الحلقة $\mathbf{Z}_6$ لدينا $e=4$ عنصر جامد غير مبتذل، لأن $e^2=4^2\equiv 4(\text{mod } 6)$، كذلك فإن $f=1-e=1-4\equiv 3(\text{mod } 6)$ هو أيضاً عنصر جامد يعامد $e=4$.

تمهيدية (١-٢-٧): [1]

لتكن R حلقة ذات عنصر وحدة, و ليكن e عنصراً جامداً من R عندئذٍ :

١) $e\in Rad\ \ R \;\Leftarrow\; e=0$.

٢) $e\in\ N_R \;\Leftarrow\; e=0$.

٣) $(er-ere)^2=0$ و $(re-ere)^2=0$ وذلك لكل r من R (من الممكن أن تكون R غير واحدية هنا).

البرهان:

١) بما أن $e\in Rad\ \ R$، فإن $(1-e)$ قابل للقلب من اليمين، بحسب (١-١-١٠)، ولذلك يوجد u من R بحيث يكون $(1-e)u=1$، و بضرب طرفي المساواة من اليسار بـ e نجد أن $e.(1-e)u=e.1$، بالتالي: $e=0$.

٢) بما أن $e\in N_R$، فإنه يوجد عدد صحيح موجب n بحيث يكون $e^n=0$، و بما أن e جامد، فإن $e^2=e$ و كذلك $e^3=e.e^2=e.e=e$، و هكذا نتابع لنجد أن $e^n=e$ بالتالي $e=0$.

٣) $(er-ere)^2 = 0$ لأن:

$$(er-ere)^2 = (er-ere)(er-ere) = erer - erere - ereer + ereere$$
$$= erer - erere - erer + erere = 0$$

- نبرهن، بنفس الاسلوب، أيضاً، على أن $(re-ere)^2 = 0$.

تمهيدية (١-٢-٨): [4]

لتكن R حلقة ذات عنصر وحدة، عندئذٍ :

١) إذا كان a,b عنصرين من الحلقة R، بحيث $a.b=1$، فإن العنصر $1-ba$ يكون عنصراً جامداً .

٢) إذا كان r عنصراً نظامياً من الحلقة R، بحيث أن $r=rr'r$ (حيث $r' \in R$)، فإن $r'r, rr'$ عنصران جامدان من R.

البرهان:

١) لنبرهن أن $1-ba$ عنصر جامد:

$$\begin{aligned}(1-ba)^2 &= (1-ba)(1-ba)\\ &= 1-ba-ba+b(ab)a\\ &= 1-ba-ba+ba\\ &= 1-ba\end{aligned}$$

٢) إن rr' جامد لأن $r'=rr'$ $(rr')^2 = (rr')(rr') = (rr'r)$

نبرهن، بنفس الأسلوب، أيضاً، على أن $r'r$ جامد.

تمهيدية (١-٢-٩): [1]

لتكن R حلقة، وليكن f عنصراً جامداً من الحلقة R، و ليكن e عنصراً من R عندئذٍ :

١) إذا كان $ef=efe$، فإن ef, fef جامدان في الحلقة R.

٢) إذا كان e جامداً بحيث $ef=efe$، فإن $e_1 = e+f-fe$ جامد في R.

٣) إذا كان e جامداً بحيث $fe=efe$، فإن $e_2 = e+f-ef$ جامد في R.

البرهان:

١) إن ef جامد لأن: $(ef)^2 = efef = eff = ef$

كذلك فإن fef جامد لأن: $(fef)^2 = feffef = fefef = feff = fef$

٢) إن e_1 جامد لأن:

$$\begin{aligned} e^2{}_1 &= (e+f-fe)(e+f-fe) \\ &= e^2+ef-efe+fe+f^2-f^2e-fe^2-fef+fefe \\ &= e+f-fe = e_1 \end{aligned}$$

٣) بنفس الأسلوب نبرهن على أن e_2 عنصر جامد.

أمثلة (١-٢-١٠):

١- لتكن الحلقة $\mathbf{Z}_{12}$، عندئذ $f=4$ جامد في $\mathbf{Z}_{12}$, وإذا كان $e \in \{0,1,3,4,6,7,9,10\}$،

فإن fef, ef جامدان في $\mathbf{Z}_{12}$، لأنهما يحققان (١) من التمهيدية السابقة.

٢- لتكن $R = M_{2\times 2}(\Re)$، عندئذٍ $e = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, $f = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$ جامدان في R،

كذلك فإن $ef = efe$، وبالتالي $e_1 = e+f-fe$ جامد في R، ونلاحظ أن:

$$e_1 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} - \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = e$$

٣- لتكن $R = M_{2\times 2}(\Re)$، عندئذٍ $e = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$, $f = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$ جامدان في R،

كذلك فإن $fe = efe$، وبالتالي العنصر $e_2 = e+f-ef$ جامد في R.

تمهيدية (١-٢-١١):[11]

إذا كانت R حلقة ذات عنصر وحدة، تحقق الشرط التالي:

(لكل r من R فإنه إما r أو $(1-r)$ قابل للقلب من اليمين (اليسار) في R)، فإن R خالية من العناصر الجامدة غير المبتذلة.

البرهان:

ليكن e عنصراً جامداً من R، عندئذٍ $e^2 = e$، أي إن $e(1-e) = 0$، وحسب الفرض فإنه إما أن يكون e أو $(1-e)$ قابلاً للقلب من اليمين (اليسار)، بالتالي إما $e = 0$ أو $e = 1$، وعليه فإن e جامد مبتذل.

نتيجة (١-٢-١٢):[11]

كل حلقة محلية و ذات عنصر وحدة، تكون خالية من العناصر الجامدة غير المبتذلة، لأن الشرط الوارد في التمهيدية السابقة يكافئ أن الحلقة الواحدية R محلية, وهناك شروط كثيرة تكافئ أن R حلقة محلية.

مبرهنة (١-٢-١٣):[11]

لتكن R حلقة ذات عنصر وحدة، عندئذ العبارات التالية متكافئة:

١- الحلقة R ايزومورفية مع جداء مباشر منتهي من الحلقات R_i، حيث $(i = 1,2,....,n)$، أي: $R \approx R_1 \otimes R_2 \otimes ..... \otimes R_n$

٢- يوجد في R عناصر جامدة مركزية متعامدة مثل $e_i \in R$، بحيث:

$$1 = \sum_{i=1}^{n} e_i \quad \text{و} \quad e_i R \approx R_i$$

٣- الحلقة R هي مجموع مباشر منته لمثاليات K_i من R، حيث $K_i \approx R_i$، أي:

$$R = K_1 \oplus K_2 \oplus .... \oplus K_n \quad ; \quad K_i \approx R_i \quad ; \quad i \in \{1,2,..,n\}.$$

مبرهنة (١-٢-١٤):[1]

لتكن R حلقة، و ليكن e, f عنصرين جامدين متعامدين من الحلقة R، عندئذٍ :

$$e_5 = e \pm f \quad , \quad e_4 = f \pm erf \quad , \quad e_3 = e \pm fre \quad , \quad e_2 = f \pm fre \quad , \quad e_1 = e \pm erf$$

جوامد في R وذلك مهما كان r من R.

البرهان:

إن e_1 عنصر جامد في R، لأن:

$$\begin{aligned} e_1^{\,2} &= (e+erf)(e+erf) \\ &= e^2 + e^2rf + erfe + erferf \\ &= e + erf + 0 + 0 = e_1 \end{aligned}$$

– وبنفس الأسلوب نبرهن أن : e_5, e_4, e_3, e_2 جوامد في R.

مبرهنة (١-٢-١٥):[1]

إذا كان e و e' عنصرين جامدين من حلقة ذات عنصر وحدة R، فإن العبارات التالية متكافئة:

(١) $e'R = eR$.

(٢) $e'e = e$ و $ee' = e'$.

(٣) يوجد عنصر r من R بحيث يكون $e' = e + er(1-e)$.

البرهان:

(١) $\Leftarrow$ (٢) لنفرض أن $e'R = eR$، ولنثبت أن $e'e = e$ و $ee' = e'$.

بما أن الحلقة R واحدية، فإن $e \in eR$، وبما أن $e'R = eR$، فإن $e = e'r$ حيث r من R، ومنه $e'e = e'e'r$، لكن e' عنصر جامد, لذلك فإن $e'e = e'r$، وينتج أن $e = e'r = e'e$ أي $e = e'e$، وبما أن $e' \in e'R = eR$، فإن $e' \in eR$ ومنه $e' = er'$ حيث $r' \in R$، ومنه $ee' = eer' = er'$، لذلك ينتج أن $e' = er' = ee'$, إذن $e' = ee'$.

(٢) $\Leftarrow$ (١) لنفرض أن $ee' = e'$ و $e'e = e$، ولنبرهن أن $e'R = eR$.

إذا كان $x \in e'R$، فإن $x \in ee'R$ لأن $e' = ee'$، لكن $ee'R \subseteq eR$ لأن $e'R \subseteq R$، إذن $x \in eR$، وبالتالي $e'R \subseteq eR$.

وإذا كان $x \in eR$، فإن $x \in e'eR$ لأن $e = e'e$، لكن $e'eR \subseteq e'R$ لأن $eR \subseteq R$، إذن $x \in e'R$، وبالتالي $eR \subseteq e'R$، إذن $eR = e'R$.

(٢) ⇐ (٣) لنفرض أن $ee' = e'$ و $e'e = e$، ولنبرهن أنه يوجد r من R بحيث $e' = e + er(1-e)$.

$$e' = e + e' - e = e + ee' - e'e = e + ee' - ee'e$$
$$= e + ee'(1-e) = e + er(1-e) \quad ; \quad r = e'$$

(٣) ⇐ (٢) لنفرض أنه يوجد عنصر r من R بحيث يكون $e' = e + er(1-e)$، و لنبرهن أن $e'e = e$ و $ee' = e'$.

بما أن $e' = e + er(1-e)$، فإن $ee' = e[e + er(1-e)] = e + er(1-e) = e'$، وكذلك $e'e = [e + er(1-e)]e = e^2 + er(e - e^2) = e$.

الخلاصة: (١) ⇔ (٢) ⇔ (٣).

مبرهنة (١-٢-١٦): [1]

لتكن R حلقة، وليكن x عنصراً ما من الحلقة R، عندئذٍ x يكون عنصراً دورياً إذا، وفقط إذا، وجد عدد صحيح موجب t بحيث يكون x^t عنصراً جامداً.

البرهان:

لزوم الشرط:

لنفرض أن x دوري، ولنبرهن أنه يوجد عدد صحيح موجب t بحيث يكون x^t عنصراً جامداً.

بما أن x دوري، فإنه يوجد عددان صحيحان موجبان m و n، بحيث أن $m > n$ و $x^m = x^n$، ولنضع $d = m - n$، فيكون $d \geq 1$ & $m = n + d$، ومنه $x^n = x^{n+d}$ وينتج عن ذلك أن: $x^{n+2d} = x^{n+d}.x^d = x^n x^d = x^{n+d} = x^n$، و بالتتابع نجد أن:

$$x^{n+sd} = x^n \quad \forall s = 1,2,3,... \quad \& \quad d \geq 1 ....(1)$$

لنأخذ $s > n$ فيكون $sd - n \geq 1$، لنضع $sd = n + r$ ثم نعوض في (1) فنجد أن: $x^{n+n+r} = x^n$، أي إن $x^{2n+r} = x^n$.

ليكن $t = n + r$ عندئذٍ x^t جامد (حيث t عدد صحيح موجب)، لأن:

$$(x^t)^2 = x^{2t} = x^{2n+2r} = x^{2n+r} x^r = x^n x^r = x^{n+r} = x^t$$

كفاية الشرط:

لنفرض وجود عدد صحيح موجب t بحيث يكون x^t عنصراً جامداً، ولنبرهن أن xدور ي.

بما أن x^t جامد، فإن $\left(x^t\right)^2 = x^t$، أي إن $x^{2t} = x^t$، فإذا وضعنا $n = t$ و $m = 2t$، نجد أن n و m عددان صحيحان موجبان يحققان $m > n$ و $x^m = x^n$، ومنه x عنصر دوري.

مبرهنة (١-٢-١٧): [1]

إذا كانت R حلقة فيها $SN_R = \{0\}$، فإن جميع العناصر الجامدة في الحلقة R ستكون مركزية.

البرهان:

إذا كان e عنصراً جامداً من R، فإن $e^2 = e$، وبالتالي مهما كان $r \in R$، فإن $(re - ere)^2 = 0$ و $(er - ere)^2 = 0$، ولذلك فإن $(re - ere) \in SN_R = \{0\}$ و $(er - ere) \in SN_R = \{0\}$، ومنه $re = ere$ و $er = ere$، وبالتالي $re = er$ أي إن e جامد مركزي.

ملاحظات (١-٢-١٨): [1]

١) إذا كانت R حلقة ذات عنصر وحدة لا تحوي قواسم للصفر، فإنها لا تحوي جوامد غير مبتذلة، لأن:

إذا كان e جامداً في R، فإن $e^2 = e$، و منه $e(1-e) = 0$، وبما أن R لا تحوي قواسم للصفر فإنه إما $e = 0$ أو $e = 1$، أي إن e جامد مبتذل.

٢) إذا كانت R حلقة ذات عنصر وحدة وبسيطة فيها $SN_R = \{0\}$، فإن R خالية من العناصر الجامدة غير المبتذلة، لأن:

إذا كان e جامداً من R،عندئذٍ e مركزياً في R بحسب (١-٢-١٧)، وبالتالي eR مثالية في R، وبالتالي إما $eR = R$ أو $eR = \{0\}$، لأن R بسيطة، ومنه $e = 0$، لأن R ذات عنصر وحدة.

نتيجة (١-٢-١٩):[11]

إذا كانت R حلقة أرتينية إلى اليمين (اليسار)، فإن:

الحلقة R محلية إذا، وفقط إذا، كانت R لاتحوي عناصر جامدة غير مبتذلة.

تعريف (١-٢-٢٠):[17]

١) إذا كانت R حلقة، و كانت I مثالية منها، فإننا نقول عن I أنها مثالية جامدة (Idempotent)، إذا حققت $I^2 = I$.

٢) نقول عن حلقة R إنها تامة الجمود (Fully Idempotent) إذا كانت كل مثالية فيها مثالية جامدة.

ملاحظات (١-٢-٢١):

(١) كل حلقة تقسيم (Division Ring) (أو حقل) هي حلقة تامة الجمود.

(٢) $\mathbf{Z}_6$ هي حلقة تامة الجمود.

الفصل الثاني

العناصر الجامدة والعناصر عديمة القوة في الحلقات $\mathbf{Z}_n$ وفي بعض الحلقات الأخرى

١.§ العناصر الجامدة في الحلقات $\mathbf{Z}_n$:

ستشير النجمة (*) فيما يأتي إلى عملنا.

***مبرهنة (٢-١-١):**

إذا كان $n = 2P$، حيث P عدد أولي يختلف عن 2، فإن الحلقة $\mathbf{Z}_n$ تحوي، فقط، عنصرين جامدين، غير مبتذلين، هما P و $P+1$، ويلاحظ أن مجموع هذين العنصرين الجامدين يطابق 1 قياس n.

البرهان:

لنبرهن أولاً على الوجود وثانياً على الوحدانية.

أولاً:

$$P^2 = P.P = \underbrace{P + P + \ldots + P}_{P \text{ مرة}} = \underbrace{2P + 2P + \ldots + 2P}_{\frac{P-1}{2} \text{ مرة}} + P$$

أي إن:

$$P^2 \equiv P(\text{mod}2P)$$

وكذلك فإن:

$$(P+1)^2 = 1 + 2P + P^2 \equiv (1+P)(\text{mod}2P)$$

وبالتالي:

$$(P+1)^2 \equiv (1+P)(\text{mod}2P)$$

ثانياً:

لنفرض أن x عنصر جامد، غير مبتذل، في الحلقة $\mathbf{Z}_n$ (قياس n)، عندئذٍ :

من جهة أولى $1 < x < 2P$، ومن جهة ثانية $x^2 \equiv x(\text{mod}2P)$ ، بالتالي $x^2 - x \equiv 0(\text{mod}2P)$ ، أي إن $2P | (x^2 - x)$ ، وبالتالي $P | x(x-1)$ ، وبما أن P عدد أولي، فإنه:

إما $P | x$ أو $P | (x-1)$ (انظر المراجع [6] و [7] و [9])

فإذا كان $P | x$ ، فإنه بالإمكان كتابة $x=P.r$ حيث $r \in \mathbf{Z}$ ، ولكن لدينا $1 < x < 2P$، بالتالي $r = 1$ ، أي إن $x=P$.

أما إذا كان $P | (x-1)$ ، فإنه بالإمكان كتابة $x=P.r+1$ حيث $r \in \mathbf{Z}$ ، ولكن لدينا $1 < x < 2P$ ، بالتالي $r = 1$ ، أي إن $x=P+1$.

ملاحظة (٢-١-٢):

إذا كان Pعدداً أولياً أكبر من 3، فإنه استناداً إلى خوارزمية القسمة يكون:

$P \equiv 1(\text{mod}3)$ أو $P \equiv 2(\text{mod}3)$.

***تمهيدية (٢-١-٣):**

إذا كان nعدداً صحيحاً موجباً من الشكل $n = q.p$ ، حيث p,q عددان أوليان مختلفان، وكان $q < p$ ، فإن الشرط اللازم حتى يكون x عنصراً جامداً في $\mathbf{Z}_n$، هو أن يكون $x \equiv 0(\text{mod}\, q)$ أو يكون $x \equiv 1(\text{mod}\, q)$.

البرهان:

لنفرض أن x عنصر جامد في $\mathbf{Z}_n$، ولنبرهن على أن $x \equiv 0(\text{mod}\, q)$ أو $x \equiv 1(\text{mod}\, q)$.

بما أن x عنصر جامد في $\mathbf{Z}_n$، فإن $x^2 \equiv x(\text{mod}\, qp)$ ، وبالتالي $x^2 - x \equiv 0(\text{mod}\, qp)$

، أي إن $q.p \mid (x^2 - x)$ ، وبالتالي $q \mid x(x-1)$ ، وبما أن q عدد أولي، فإنه:

إما $q \mid x$ أو $q \mid (x-1)$.

فإذا كان $q \mid x$ ، فإن $x = qr$ حيث $r \in \mathbf{Z}$ ، وبالتالي $x \equiv 0(\text{mod}\, q)$.

وا ٕذا كان $q \mid (x-1)$ ، فإن $x = qr + 1$ حيث $r \in Z$ ، وبالتالي $x \equiv 1(\text{mod}\, q)$.

ملاحظة (٢-١-٤):

إن عكس التمهيدية السابقة ليس من الضروري أن يكون صحيحاً، لأنه إذا أخذنا الحلقة $\mathbf{Z}_{5\times 11} = \mathbf{Z}_{55}$ ، ($p = 11$ و $q = 5$)، فإننا نجد، مثلاً ، $x = 46 \in \mathbf{Z}_{55}$ و $x \equiv 1(\text{mod}\, 5)$

ولكن مع ذلك فإن $x = 46$ليس عنصراً جامداً في $\mathbf{Z}_{5\times 11} = \mathbf{Z}_{55}$.

***مبرهنة (٢-١-٥):**

إذا كان n=3P، حيث P عدد أولي أكبر من 3، فإن الحلقة $\mathbf{Z}_n$ تحوي، فقط، عنصر ين جامدين، غير مبتذلين وفق ما يأتي:

١- عندما $P \equiv 1(\text{mod}3)$ هما P و $2P+1$.

٢- عندما $P \equiv 2(\text{mod}3)$ هما $P+1$ و $2P$.

ويلاحظ أن مجموع العنصرين الجامدين في كل من الحالتين السابقتين يطابق 1 قياس n .

البرهان:

لنبرهن أولاً على الوجود وثانياً على الوحدانية.

أولاً:

١- عندما $P \equiv 1(\text{mod}3)$ ، فإنه بالإمكان كتابة $P = 1 + 3r$ حيث $r \in \mathbf{Z}$ ، وبضرب الطرفين بـ P نجد أن $P^2 = P + 3P.r$ ، أي إن $P^2 \equiv P(\text{mod}3P)$ ، إذاً P جامد قياس n .

وكذلك فإن:

$$(2P+1)^2 = 4P^2 + 4P + 1 \equiv (4P + 4P + 1)(\text{mod} 3P)$$
$$\equiv (2P+1)(\text{mod} 3P)$$

إذاً $(2P+1)$ جامد قياس $n = 3P$.

٢- عندما $P \equiv 2(\text{mod} 3)$، فإنه بالإمكان كتابة $P = 2 + 3r$ حيث $r \in \mathbf{Z}$، وبضرب الطرفين بـ P نجد أن $P^2 = 2P + 3P.r$، أي إن $P^2 \equiv 2P(\text{mod} 3P)$، وبالتالي:

$$(2P)^2 = 4P^2 \equiv (8P)(\text{mod} 3P)$$
$$\equiv (2P)(\text{mod} 3P)$$

إذاً $(2P)$ جامد قياس $n = 3P$.

وكذلك:

$$(P+1)^2 = P^2 + 2P + 1 \equiv (2P + 2P + 1)(\text{mod } 3P)$$
$$\equiv (P+1)(\text{mod } 3P)$$

وبالتالي $(P+1)$ جامد قياس $n = 3P$.

ثانياً:

لنفرض أن M هي مجموعة جميع العناصر الجامدة غير المبتذلة والتي رأيناها في $\mathbf{Z}_n$، أي إن:

$$M = \{P, 2P, P+1, 2P+1\}$$

ولنفرض أن x عنصر جامد غير مبتذل في $\mathbf{Z}_n$ عندئذٍ من جهة أولى $1 < x < 3P$ ومن جهة ثانية $x^2 \equiv x(\text{mod} 3P)$، بالتالي $x^2 - x \equiv 0(\text{mod} 3P)$، أي إن $3P \mid (x^2 - x)$، وبالتالي $P \mid x(x-1)$، وبما أن P عدد أولي، فإنه:

إما $P \mid x$ أو $P \mid (x-1)$

* - فإذا كان $P \mid x$، فإنه بالإمكان كتابة $x = P.r$ حيث $r = 1$ أو $r = 2$، لأن $1 < x < 3P$، وبالتالي $x \in M$.
* -وإذا كان $P \mid (x-1)$، فإنه بالإمكان كتابة $x = P.r + 1$ حيث $r = 1$ أو $r = 2$، لأن $1 < x < 3P$، وبالتالي $x \in M$.

وبالاستفادة من التمهيدية (٢-١-٣) نجد المطلوب.

ملاحظة (٢-١-٦):

إذا كان P عدداً أولياً ما، أكبر من 5، فإنه استناداً إلى خوارزمية القسمة يكون: $P \equiv 1(\text{mod } 5)$ أو $P \equiv 2(\text{mod} 5)$ أو $P \equiv 3(\text{mod } 5)$ أو $P \equiv 4(\text{mod } 5)$.

***مبرهنة (٢-١-٧):**

إذا كان $n = 5P$، حيث P عدد أولي أكبر من 5، فإن الحلقة $\mathbf{Z}_n$ تحوي، فقط، عنصرين جامدين، غير مبتذلين، وفق ما يأتي:

١- عندما $P \equiv 1(\text{mod } 5)$ هما P و $4P+1$.

٢- عندما $P \equiv 2(\text{mod } 5)$ هما $3P$ و $2P+1$.

٣- عندما $P \equiv 3(\text{mod } 5)$ هما $2P$ و $3P+1$.

٤- عندما $P \equiv 4(\text{mod } 5)$ هما $4P$ و $P+1$.

ويلاحظ أن مجموع العنصرين الجامدين في كل من الحالات السابقة يطابق 1 قياس n.

البرهان:

لنبرهن أولاً على الوجود وثانياً على الوحدانية.

أولاً:

١- إذا كان $P \equiv 1(\text{mod } 5)$، فإنه بالإمكان كتابة $P = 1 + 5r$ حيث $r \in \mathbf{Z}$، وبضرب الطرفين بـ P، نجد أن:

$P^2 = P + 5P.r$ أي إن $P^2 \equiv P(\text{mod } 5P)$، إذاً P جامد في الحلقة $\mathbf{Z}_n$ (جامد قياس n).

وأيضاً:

$$(4P+1)^2 = 16P^2 + 8P + 1 \equiv (24P+1)(\text{mod } 5P)$$
$$\equiv (4P+1)(\text{mod } 5P)$$

وبالتالي $(4P+1)$ جامد قياس n.

٢- إذا كان $P \equiv 2(\text{mod } 5)$، فإنه بالإمكان كتابة $P = 2 + 5r$ حيث $r \in \mathbf{Z}$، وبضرب الطرفين بـ P نجد أن $P^2 = 2P + 5P.r$، أي إن:

$$P^2 \equiv 2P(\text{mod } 5P)$$

وعليه فإن:

$$(3P)^2 = 9P^2 \equiv 18P(\text{mod } 5P)$$
$$\equiv 3P(\text{mod } 5P)$$

وبالتالي $3P$ جامد قياس n.

وأيضاً :

$$(2P+1)^2 = 4P^2 + 4P + 1 \equiv (12P+1)(\text{mod } 5P)$$
$$\equiv (2P+1)(\text{mod } 5P)$$

أي إن $(2P+1)$ جامد قياس n.

٣- إذا كان $P \equiv 3(\text{mod } 5)$ ، فإنه بالإمكان كتابة $P = 3+5r$ حيث $r \in \mathbf{Z}$ ،
وبضرب الطرفين بـ P نجد أن $P^2 = 3P + 5P.r$ ، أي إن:

$$P^2 \equiv 3P(\text{mod } 5P)$$

وعليه فإن:

$$(2P)^2 = 4P^2 \equiv 12P(\text{mod } 5P)$$
$$\equiv 2P(\text{mod } 5P)$$

أي إن $(2P)$ جامد قياس n.

وكذلك فإن:

$$(3P+1)^2 = 9P^2 + 6P + 1 \equiv (33P+1)(\text{mod } 5P)$$
$$\equiv (3P+1)(\text{mod } 5P)$$

أي إن $(3P+1)$ جامد قياس n.

٤- إذا كان $P \equiv 4(\text{mod } 5)$ ، فإنه بالإمكان كتابة $P = 4+5r$ حيث $r \in \mathbf{Z}$ ،
وبضرب الطرفين بـ P نجد أن $P^2 = 4P + 5P.r$ ، أي إن:

$$P^2 \equiv 4P(\text{mod } 5P)$$

وعليه فإن:

$$(4P)^2 = 16P^2 \equiv 64P(\text{mod } 5P)$$
$$\equiv 4P(\text{mod } 5P)$$

أي إن $(4P)$ جامد قياس n.

وكذلك فإن:

$$(P+1)^2 = P^2 + 2P + 1 \equiv (6P+1)(\text{mod } 5P)$$
$$\equiv (P+1)(\text{mod } 5P)$$

أي إن $(P+1)$ جامد قياس n.

ثانياً :

لنفرض أن M هي مجموعة جميع العناصر الجامدة غير المبتذلة والتي رأيناها في $\mathbf{Z}_n$ ،
أي إن:

$$M = \{P, 2P, 3P, 4P, P+1, 2P+1, 3P+1, 4P+1\}$$

ولنفرض أن x عنصر جامد غير مبتذل في $\mathbf{Z}_n$ عندئذٍ من جهة أولى $1 < x < 5P$، ومن جهة ثانية $x^2 \equiv x(\bmod 5P)$، بالتالي $x^2 - x \equiv 0(\bmod 5P)$، أي إن $5P \mid (x^2 - x)$، وبالتالي $P \mid x(x-1)$، وبما أن P عدد أولي، فإنه:

إما $P \mid x$ أو $P \mid (x-1)$

- فإذا كان $P \mid x$، فإنه بالإمكان كتابة $x = P.r$ حيث $r = 1$ أو $r = 2$ أو $r = 3$ أو $r = 4$ ، لأن $1 < x < 5P$، ولذلك فإن $x \in M$.

-وإذا كان $P \mid (x-1)$، فإنه بالإمكان كتابة $x = P.r + 1$ حيث $r = 1$ أو $r = 2$ أو $r = 3$ أو $r = 4$، لأن $1 < x < 5P$، ولذلك فإن $x \in M$.

وبالاستفادة من التمهيدية (٢-١-٣) نجد المطلوب.

***مبرهنة (٢-١-٨):**

لنفرض أن $n = q.p$، حيث p,q عددان أوليان مختلفان، ولنفرض أن $q < p$، عندئذٍ :

إذا كان $p \equiv \alpha(\bmod q)$ حيث $\alpha \in \mathbf{Z}$، فإن الحلقة $\mathbf{Z}_n$ تحوي، فقط، عنصرين جامدين، غير مبتذلين، هما $\alpha^{\varphi(q)-1}P$ و $1 - \alpha^{\varphi(q)-1}P$ حيث φ هو تابع أولر.

ويلاحظ أن مجموع العنصرين الجامدين السابقين يطابق 1 قياس $n = q.p$.

البرهان:

لنبرهن أولاً الوجود وثانياً على الوحدانية.

أولاً:

بما أن $p \equiv \alpha(\bmod q)$ و بما أن $\gcd(p,q) = \gcd(\alpha,q) = 1$، فإنه استناداً إلى مبرهنة أولر يكون $\alpha^{\varphi(q)} \equiv 1(\bmod q)$، وبالتالي $\alpha^{\varphi(q)-1}.p \equiv 1(\bmod q)$، ومنه $\alpha^{\varphi(q)-1}.p = 1 + qr$ حيث $r \in \mathbf{Z}$، وبضرب الطرفين بـ $\alpha^{\varphi(q)-1}.p$ نجد أن:

$$(\alpha^{\varphi(q)-1})^2.p^2 = \alpha^{\varphi(q)-1}p + qpr\alpha^{\varphi(q)-1}$$

وبالتالي $(\alpha^{\varphi(q)-1}.p)^2 \equiv (\alpha^{\varphi(q)-1}.p)(\bmod qp)$، أي إن $\alpha^{\varphi(q)-1}.p$ عنصر جامد قياس $n = q.p$.

أما البرهان على أن $1 - \alpha^{\varphi(q)-1}P$ جامد قياس $n = q.p$ فهو واضح.

ثانياً:

ليكن x عنصراً جامداً، غير مبتذل، في الحلقة $\mathbf{Z}_n$ عندئذٍ :

من جهة أولى يكون $x^2 \equiv x(\bmod qp)$، ومن جهة ثانية، واستناداً إلى التمهيدية (٢-١-٣)، يكون $x \equiv 0(\bmod q)$ أو $x \equiv 1(\bmod q)$.

بما أن $x^2 \equiv x(\bmod qp)$ ، فإن $x^2 - x \equiv 0(\bmod qp)$ ، وبالتالي $qp \mid x(x-1)$ ،
أي إن $p \mid x(x-1)$ ، وبما أن p عدد أولي، فإنه:

إما $p \mid x$ أو $p \mid (x-1)$

*- عندما $x \equiv 0(\bmod q)$ ، فإنه:

- إذا كان $p \mid x$ ، فإنه بالإمكان كتابة $x = pr$ حيث $1 < r < q$ ، وبالتالي $pr \equiv 0(\bmod q)$ ، أي إن $q \mid pr \,\&\, r < q$ ، وبالتالي $q \mid p$ ، وبما أن q, p عددان أوليان مختلفان، فإن هذا مرفوض.

- أما إذا كان $p \mid (x-1)$ ، فإنه بالإمكان كتابة $x = pr + 1$ حيث $1 < r < q$ ، وبالتالي $pr + 1 \equiv 0(\bmod q)$ ، أي إن $pr \equiv -1(\bmod q)$، واستناداً إلى الفرض $p \equiv \alpha(\bmod q)$ ، واستناداً إلى مبرهنة أولر $\alpha^{\varphi(q)} \equiv 1(\bmod q)$ ، ولذلك فإن $\alpha^{\varphi(q)-1}.p \equiv 1(\bmod q)$.

الآن، بما أننا وجدنا $pr \equiv -1(\bmod q)$ ، فبضرب الطرفين بـ $\alpha^{\varphi(q)-1}$ نجد أن:

$$\alpha^{\varphi(q)-1} pr \equiv -\alpha^{\varphi(q)-1}(\bmod q)$$

ولكن $\alpha^{\varphi(q)-1} p \equiv 1(\bmod q)$ ، بالتالي $r \equiv -\alpha^{\varphi(q)-1}(\bmod q)$ ، أي إن $r \equiv (q - \alpha^{\varphi(q)-1})(\bmod q)$ ، وبالتالي $q \mid [r - (q - \alpha^{\varphi(q)-1})]$ ، أي إنه بالإمكان كتابة $r = (q - \alpha^{\varphi(q)-1}) + qs$ حيث $s \in \mathbf{Z}$ ، وبضرب الطرفين بـ p نجد أن $pr = p(q - \alpha^{\varphi(q)-1}) + pqs$ ، وبالتالي:

$$pr \equiv p(q - \alpha^{\varphi(q)-1})(\bmod qp)$$

وبما أن $1 \equiv 1(\bmod qp)$ ، فإنه بجمع التطابقين نجد أن:

$$x \equiv [p(q - \alpha^{\varphi(q)-1}) + 1](\bmod qp)$$
$$\equiv (1 - \alpha^{\varphi(q)-1}.p)(\bmod qp)$$

وبالتالي x يكون أحد الجامدين الواردين في (أولاً).

*- أما عندما $x \equiv 1(\bmod q)$ ، فإنه:

- إذا كان $p \mid x$ ، فإن بالإمكان كتابة $x = pr$ حيث $1 < r < q$ ، وبالتالي $pr \equiv 1(\bmod q)$ ، ولدينا استناداً إلى الفرض وإلى مبرهنة أولر $\alpha^{\varphi(q)-1}.p \equiv 1(\bmod q)$ ، وبالتالي نجد $pr \equiv p\alpha^{\varphi(q)-1}(\bmod q)$ ، وبما أن $\gcd(q, p) = 1$ ، فإنه بالإمكان قسمة طرفي التطابق السابق على p نجد أن:

$$r \equiv \alpha^{\varphi(q)-1}(\bmod q)$$

أي إن $q\,|\,(r-\alpha^{\varphi(q)-1})$ ، بالتالي بالإمكان كتابة $r=\alpha^{\varphi(q)-1}+qs$ حيث $s\in Z$ ، وبضرب الطرفين بـ p نجد أن $pr=p\alpha^{\varphi(q)-1}+qps$ ، أي إن $x\equiv p\alpha^{\varphi(q)-1}(\bmod qp)$ ، وبالتالي x يكون أحد الجامدين الواردين في (أولاً).

– أما إذا كان $p\,|\,(x-1)$ ، فإنه بالإمكان كتابة $x=pr+1$ حيث $1<r<q$، وبالتالي $pr+1\equiv 1(\bmod q)$ ، أي $pr\equiv 0(\bmod q)$ ، بالتالي $q\,|\,pr\ \&\ 1<r<q$، أي إن $q\,|\,p$ ، وبما أن q,p عددان أوليان مختلفان،و هذا مرفوض.

تمهيدية (٢-١-٩):

ليكن p عدداً أولياً أكبر من 3، عندئذ $p\equiv 1(\bmod 6)$ أو $p\equiv 5(\bmod 6)$.

البرهان:

بما أن p عددٌ أولي أكبر من 3، فإن $\gcd(p,6)=1$.

إذا كان $p\equiv\alpha(\bmod 6)$ ، فإن $\alpha\in\{0,1,2,3,4,5\}$ ، بالاعتماد على أن $\gcd(\alpha,6)=1$ ، فإن $\alpha=1$ أو $\alpha=5$.

***مبرهنة (٢-١-١٠):**

إذا كان $n=2.3.P$، حيث P عدد أولي أكبر من 3، فإن الحلقة $\mathbf{Z}_n$ تحوي، فقط، ستة عناصر جامدة، غير مبتذلة، وفق ما يأتي:

١- عندما $P\equiv 1(\bmod 6)$ هي $P,\ 2P+1,\ 3P,\ 3P+1,\ 4P,\ 5P+1$.

٢- عندما $P\equiv 5(\bmod 6)$ هي $P+1,\ 2P\ ,\ 3P,\ 3P+1,\ 4P+1,\ 5P$.

البرهان:

لنبرهن أولاً على الوجود وثانياً على الوحدانية.

أولاً:

١- عندما $P\equiv 1(\bmod 6)$ ، فإنه بالإمكان كتابة $P=6r+1$ حيث $r\in\mathbf{Z}$ ، وبضرب الطرفين بـ P نجد أن $P^2=6P.r+P$ ، أي إن $P^2\equiv P(\bmod 6P)$ ، إذاً P جامد قياس $n=2.3.P$.

وكذلك فإن:

$$(2P+1)^2=4P^2+4P+1$$

أي إن:

$$(2P+1)^2\equiv(4P+4P+1)(\bmod 6P)$$
$$\equiv(2P+1)(\bmod 6P)$$

وبالتالي $(2P+1)$ جامد قياس $n=2.3.P$.

أيضاً :

$$(3P)^2 = 9P^2 \equiv 9P(\text{mod } 6P)$$
$$\equiv 3P(\text{mod } 6P)$$

وبالتالي $3P$ جامد قياس $n = 2.3.P$.

وكذلك فإن:

$$(3P+1)^2 = 9P^2 + 6P + 1 \equiv (15P+1)(\text{mod } 6P)$$
$$\equiv (3P+1)(\text{mod } 6P)$$

بالتالي $(3P+1)$ جامد قياس $n = 2.3.P$.

وأيضاً :

$$(4P)^2 = 16P^2 \equiv 16P(\text{mod } 6P)$$
$$\equiv 4P(\text{mod } 6P)$$

بالتالي $4P$ جامد قياس $n = 2.3.P$.

وكذلك أيضاً :

$$(5P+1)^2 = 25P^2 + 10P + 1 \equiv (35P+1)(\text{mod } 6P)$$
$$\equiv (5P+1)(\text{mod } 6P)$$

بالتالي $(5P+1)$ جامد قياس $n = 2.3.P$.

٢- نبرهن، بنفس المناقشة السابقة، على أنه عندما $P \equiv 5(\text{mod } 6)$ يكون كل من $P+1,\ 2P$ $3P,\ 3P+1,\ 4P+1,\ 5P$ عنصراً جامداً ، غير مبتذل، في الحلقة $\mathbf{Z}_n$.

ثانياً :

لنفرض M هي مجموعة جميع العناصر الجامدة وغير المبتذلة التي رأيناها في $\mathbf{Z}_n$، أي إن:

$$M = \{x \in \mathbf{Z}_n \ ;\ x \in \{P, 2P+1, 3P, 3P+1, 4P, 5P+1\} \ \ if \ \ P \equiv 1(\text{mod}6)$$
$$x \in \{P+1, 2P, 3P, 3P+1, 4P+1, 5P\} \ \ if \ \ P \equiv 5(\text{mod}6)\}$$

ولنفرض أن x عنصر جامد، غير مبتذل، في الحلقة Z_n، فيكون $x^2 \equiv x(\text{mod } 6P)$، أي إن $x^2 - x \equiv 0(\text{mod } 6P)$، وبالتالي $6P \mid x(x-1)$، أي إن $p \mid x(x-1)$، وبما أن p عدد أولي، فإنه إما $p \mid x$ أو $p \mid (x-1)$.

إذا كان $P \mid x$، فإنه بالإمكان كتابة $x = P.r$، وبما أن $1 < x < 6P$، فإن $1 < r < 6$، بالتالي $x \in M$.

وإذا كان $P \mid (x-1)$، فإنه بالإمكان كتابة $x = P.r + 1$، وبما أن $1 < x < 6P$، فإن $1 < r < 6$، بالتالي $x \in M$.

بالإضافة إلى ذلك، يمكن بسهولة البرهان على ما يأتي:

- العناصر $P, 2P+1, 4P, 5P+1$ ليست جامدة في الحالة $P \equiv 5 (\bmod 6)$.
- العناصر $P+1, 2P, 4P+1, 5P$ ليست جامدة في الحالة $P \equiv 1 (\bmod 6)$.

فيتم المطلوب.

تمهيدية (٢-١-١١):

ليكن P عدداً أولياً أكبر من 5 عندئذٍ :

إذا كان $P \equiv \alpha (\bmod 15)$، فإن $\alpha \in \{1,2,4,7,8,11,13,14\}$.

البرهان:

بما أن P عدد أولي اكبر من 5، فإن $(P,15) = 1$.

وبما أن $P \equiv \alpha (\bmod 15)$، فإن $(\alpha,15) = 1$ و $0 < \alpha < 15$، وعليه فإن:

$$\alpha \in \{1,2,4,7,8,11,13,14\}$$

***مبرهنة (٢-١-١٢):**

إذا كان $n = 3.5.P$، حيث P عدد أولي أكبر من 5، فإن الحلقة $\mathbf{Z}_n$ تحوي، فقط، ستة عناصر جامدة غير مبتذلة، وفق ما يأتي:

١- عندما $P \equiv 1 (\bmod 15)$ تكون مجموعة هذه العناصر هي:

$$M_1 = \{P, 5P+1, 6P, 9P+1, 10P, 14P+1\}$$

٢- عندما $P \equiv 2 (\bmod 15)$ تكون مجموعة هذه العناصر هي:

$$M_2 = \{3P, 5P, 7P+1, 8P, 10P+1, 12P+1\}$$

٣- عندما $P \equiv 4 (\bmod 15)$ تكون مجموعة هذه العناصر هي:

$$M_3 = \{4P, 5P+1, 6P+1, 9P, 10P, 11P+1\}$$

٤- عندما $P \equiv 7 (\bmod 15)$ تكون مجموعة هذه العناصر هي:

$$M_4 = \{2P+1, 3P, 5P+1, 10P, 12P+1, 13P\}$$

٥- عندما $P \equiv 8 (\bmod 15)$ تكون مجموعة هذه العناصر هي:

$$M_5 = \{2P, 3P+1, 5P, 10P+1, 12P, 13P+1\}$$

٦- عندما $P \equiv 11 (\bmod 15)$ تكون مجموعة هذه العناصر هي:

$$M_6 = \{4P+1, 5P, 6P, 9P+1, 10P+1, 11P\}$$

٧- عندما $P \equiv 13 (\bmod 15)$ تكون مجموعة هذه العناصر هي:

$$M_7 = \{3P+1, 5P+1, 7P, 8P+1, 10P, 12P\}$$

٨- عندما $P \equiv 14 (\bmod 15)$ تكون مجموعة هذه العناصر هي:

$$M_8 = \{P+1, 5P, 6P+1, 9P, 10P+1, 14P\}$$

البرهان:

نحصل، بإتباع الأسلوب نفسه المتبع في المبرهنات السابقة، على البرهان.

***تمهيدية (٢-١-١٣):**

إذا كان n عدداً صحيحاً موجباً من الشكل $n = qpr$، حيث p, q, r أعداد أولية مختلفة، وكان $p < q < r$، فإن الشرط اللازم حتى يكون x عنصراً جامداً في $\mathbf{Z}_n$، هو أن يكون $x \equiv 0 (\bmod qr)$ أو $x \equiv 1 (\bmod qr)$ أو $x \equiv 0 (\bmod qp)$ أو $x \equiv 1 (\bmod qp)$ أو $x \equiv 0 (\bmod pr)$ أو $x \equiv 1 (\bmod pr)$.

البرهان:

لنفرض أن x عنصر جامد في $\mathbf{Z}_n$ (جامد قياس n). عندئذٍ $x^2 \equiv x (\bmod pqr)$، وبالتالي $x^2 - x \equiv 0 (\bmod pqr)$، أي إن $pqr \mid (x^2 - x)$، وبالتالي $pqr \mid x(x-1)$، وبما أن $\gcd(x, x-1) = 1$، فإنه بالاعتماد على أن كلاً من p, q, r عدد أولي، تكون إحدى الحالات التالية محققة:

١- إما $qr \mid x$ أو $qr \mid (x-1)$.

٢- إما $qp \mid x$ أو $qp \mid (x-1)$.

٣- إما $pr \mid x$ أو $pr \mid (x-1)$.

١- إذا كان $qr \mid x$، فإن $x = qrk$ حيث $k \in \mathbf{Z}$، وبالتالي $x \equiv 0 (\bmod qr)$.

وإذا كان $qr \mid (x-1)$، فإن $x = qrk + 1$ حيث $k \in \mathbf{Z}$، وبالتالي $x \equiv 1 (\bmod qr)$.

بالمثل نبرهن باقي الحالات.

***مبرهنة (٢-١-١٤):**

لتكن الحلقة $\mathbf{Z}_n$، بحيث $n = p.q.r$ و p, q, r أعداد أولية مختلفة، ولتكن $p \equiv \alpha (\bmod qr)$ و $q \equiv \beta (\bmod pr)$ و $r \equiv \gamma (\bmod qp)$ عندئذٍ الحلقة $\mathbf{Z}_n$ تحوي، فقط، ستة عناصر جامدة، غير مبتذلة، هي:

$$\alpha^{\varphi(qr)-1}.p \quad \text{و} \quad 1-\alpha^{\varphi(qr)-1}p$$

$$\beta^{\varphi(pr)-1}.q \quad \text{و} \quad 1-\beta^{\varphi(pr)-1}q$$

$$\gamma^{\varphi(qp)-1}.r \quad \text{و} \quad 1-\gamma^{\varphi(qp)-1}r$$

ويلاحظ أن مجموع العنصرين الجامدين في كل من الحالات السابقة يطابق 1 قياس n.

البرهان:

لنبرهن أولاً على الوجود وثانياً على الوحدانية.

أولاً :

بما أن $p \equiv \alpha (\bmod qr)$ ، و بما أن كلاً من q, p, r أعداد أولية مختلفة، فإن: $\gcd(p, qr) = \gcd(\alpha, qr) = 1$، وبالتالي استناداً إلى مبرهنة أولر يكون $\alpha^{\varphi(qr)} \equiv 1 (\bmod qr)$ ، بالتالي $\alpha^{\varphi(qr)-1}.p \equiv 1 (\bmod qr)$ ، ومنه $\alpha^{\varphi(qr)-1}.p = 1 + qr\lambda$ حيث $\lambda \in \mathbf{Z}$ ، وبضرب الطرفين بـ $\alpha^{\varphi(qr)-1}.p$ نجد أن:

$$(\alpha^{\varphi(qr)-1})^2.p^2 = \alpha^{\varphi(qr)-1}p + qpr\lambda\alpha^{\varphi(qr)-1}$$

وبالتالي $(\alpha^{\varphi(qr)-1}.p)^2 \equiv (\alpha^{\varphi(qr)-1}.p)(\bmod qpr)$ ، أي إن $\alpha^{\varphi(qr)-1}.p$ عنصر جامد في الحلقة $\mathbf{Z}_n$ (جامد قياس n).

أما برهان أن $1-\alpha^{\varphi(qr)-1}.p$ عنصر جامد في الحلقة Z_n ، فهو واضح.

وبنفس الطريقة نبرهن على أن كلاً من $\beta^{\varphi(pr)-1}.q$ ، $1-\beta^{\varphi(pr)-1}.q$ ، $\gamma^{\varphi(qp)-1}.r$ ، $1-\gamma^{\varphi(qp)-1}.r$ هو عنصر جامد في الحلقة $\mathbf{Z}_n$ (جامد قياس n).

وهو المطلوب أولاً.

ثانياً :

لنفرض M هي مجموعة جميع العناصر الجامدة وغير المبتذلة التي رأيناها في $\mathbf{Z}_n$ ، أي إن:

$$M = \{1-\alpha^{\varphi(qr)-1}.p, \alpha^{\varphi(qr)-1}p, \beta^{\varphi(pr)-1}q,$$
$$1-\beta^{\varphi(pr)-1}.q, 1-\gamma^{\varphi(pq)-1}.r, \gamma^{\varphi(pq)-1}r\}$$

ليكن x عنصراً جامداً ، غير مبتذل، من $\mathbf{Z}_n$ عندئذٍ :

من جهة أولى يكون $x^2 \equiv x (\bmod qpr)$، ومن جهة ثانية، واستناداً إلى التمهيدية (٢-١-١٣)، يكون $x \equiv 0 (\bmod qr)$ أو $x \equiv 1 (\bmod qr)$ أو $x \equiv 0 (\bmod qp)$ أو $x \equiv 1 (\bmod qp)$ أو $x \equiv 0 (\bmod pr)$ أو $x \equiv 1 (\bmod pr)$.

بما أن $x^2 \equiv x (\bmod qpr)$ ، فإن $x^2 - x \equiv 0 (\bmod qpr)$ ، وبالتالي $qpr \mid x(x-1)$ أي إن $p \mid x(x-1)$ ، وبما أن p عدد أولي، فإنه:

إما $p \mid x$ أو $p \mid (x-1)$

- عندما $x \equiv 0 (\bmod qr)$ ، فإنه:

- إذا كان $p \mid x$ ، فإنه بالإمكان كتابة $x = pl$ حيث $l \in Z$ ، وبالتالي $pl \equiv 0 (\bmod qr)$ ، أي إن $pl = qr.s$ حيث $s \in \mathbf{Z}$ ، و بضرب الطرفين بـ $\alpha^{\varphi(qr)-1}$ ، نجد أن $\alpha^{\varphi(qr)-1}pl = qr.\alpha^{\varphi(qr)-1}s$ ، أي إن $\alpha^{\varphi(qr)-1}pl = qr.s'$ حيث $s' = \alpha^{\phi(qr)-1}s \in \mathbf{Z}$ ، وبما أن $\alpha^{\varphi(qr)-1}p \equiv 1 (\bmod qr)$ ، فإنه يكون $l = qr.s''$ حيث $s'' \in \mathbf{Z}$ ، وبضرب الطرفين بـ p نجد $pl = pqr.s''$ ، أي إن $x = pqr.s''$ ، وبالتالي

$x \equiv 0 (\mod qpr)$ ، وهذا يتناقض مع فرضنا بأن x عنصر جامد، غير مبتذل، و هذا مرفوض.

- أما إذا كان $p \mid (x-1)$ ، فإنه بالإمكان كتابة $x = pl + 1$ حيث $l \in \mathbf{Z}$، وبالتالي $pl + 1 \equiv 0 (\mod qr)$ ، أي إن $pl \equiv -1 (\mod qr)$.

بضرب طرفي التطابق بـ $\alpha^{\varphi(qr)-1}$ نجد:

$$\alpha^{\varphi(qr)-1} pl \equiv -\alpha^{\varphi(qr)-1} (\mod qr)$$

بالتالي:

$$\alpha^{\varphi(qr)-1} pl = -\alpha^{\varphi(qr)-1} + qr.s \text{ حيث } s \in \mathbf{Z}$$

وبما أن $\alpha^{\varphi(qr)-1} p \equiv 1 (\mod qr)$ ، فإن $\alpha^{\varphi(qr)-1} p = 1 + qrd ; d \in \mathbf{Z}$

$$(1 + qrd) l = -\alpha^{\varphi(qr)-1} + qr.s$$

$$l + lqrd = -\alpha^{\varphi(qr)-1} + qr.s$$

$$l = -\alpha^{\varphi(qr)-1} + qr(s + ld)$$

$$l = -\alpha^{\varphi(qr)-1} + qr.s' ; s' \in \mathbf{Z}$$

وبضرب الطرفين بـ p نجد أن:

$$pl = -\alpha^{\varphi(qr)-1} p + pqr.s'$$

أي إن $pl + 1 = 1 - \alpha^{\varphi(qr)-1} p + pqr.s'$ ، وبالتالي:

$x \equiv (1 - \alpha^{\varphi(qr)-1}.p)(\mod qpr)$ ، أي إن $x \in M$.

- أما عندما $x \equiv 1 (\mod qr)$ ، فإنه:

- إذا كان $p \mid x$ ، فإنه بالإمكان كتابة $x = pl$ حيث $l \in \mathbf{Z}$ ، وبالتالي $pl \equiv 1 (\mod qr)$ ، وبضرب طرفي التطابق بـ $\alpha^{\varphi(qr)-1}$ نجد:

$$\alpha^{\varphi(qr)-1} pl = \alpha^{\varphi(qr)-1} (\mod qr)$$

وبما أن $\alpha^{\varphi(qr)-1} p \equiv 1 (\mod qr)$ ، فإن $l = \alpha^{\varphi(qr)-1} (\mod qr)$ ، وبالتالي $l = \alpha^{\varphi(qr)-1} + qr.s$ ، حيث $s \in \mathbf{Z}$ ، وبضرب الطرفين بـ p نجد $pl = \alpha^{\varphi(qr)-1} p + pqr.s$ ، أي إن:

$$x = \alpha^{\varphi(qr)-1} p + pqr.s$$

وبالتالي:

$x \equiv \alpha^{\varphi(qr)-1} p (\mod qpr)$ أي إن $x \in M$.

- أما إذا كان $p|(x-1)$ ، فإنه بالإمكان كتابة $x = pl+1$ حيث $l \in \mathbf{Z}$، وبالتالي $pl+1 \equiv 1 (\bmod qr)$ ، أي إن $pl \equiv 0 (\bmod qr)$ ، أي إن $pl = qr.s$ حيث $s \in \mathbf{Z}$، و بضرب الطرفين بـ $\alpha^{\varphi(qr)-1}$ نجد $\alpha^{\varphi(qr)-1} pl = qr.\alpha^{\varphi(qr)-1} s$ ، أي إن:
$\alpha^{\varphi(qr)-1} pl = qr.s'$ حيث $s' \in \mathbf{Z}$.

وبما أن $\alpha^{\varphi(qr)-1} p \equiv 1 (\bmod qr)$ ، فإنه يكون $l = qr.s''; s'' \in \mathbf{Z}$ ، وبضرب الطرفين بـ p نجد $pl = pqr.s''$ ، أي إن $x = 1 + pqr.s''$ ، وبالتالي $x \equiv 1 (\bmod qpr)$ ، وهذا يتناقض مع فرضنا بأن x عنصر جامد، غير مبتذل،و هذا مرفوض.

وبمناقشة مماثلة نجد أنه:

- عندما $x \equiv 0 (\bmod pr)$ و $q|(x-1)$ يكون:
$x \equiv (1-\beta^{\varphi(pr)-1}.q)(\bmod qpr)$ ، أي إن $x \in M$.
- وعندما $x \equiv 1 (\bmod pr)$ و $q|x$ يكون:
$x \equiv \beta^{\varphi(pr)-1} q (\bmod qpr)$ ، أي إن $x \in M$.
- وعندما $x \equiv 0 (\bmod pq)$ و $r|(x-1)$ يكون:
$x \equiv (1-\gamma^{\varphi(pq)-1}.r)(\bmod qpr)$ ، أي إن $x \in M$.
- وعندما $x \equiv 1 (\bmod pq)$ و $r|x$ يكون:
$x \equiv \gamma^{\varphi(pq)-1} r (\bmod qpr)$ ، أي إن $x \in M$.

بالتالي إذا كان x عنصراً جامداً ما من $\mathbf{Z}_n$ ، وغير مبتذل، فإن $x \in M$.
وهو المطلوب ثانياً.

***مبرهنة (٢-١-١٥):**

لتكن الحلقة $\mathbf{Z}_n$ ، بحيث $n = P_1.P_2...P_k$ و $P_1, P_2, .., P_k$ أعداد أولية مختلفة، عندئذ تحوي الحلقة $\mathbf{Z}_n$ ، فقط، $2^k - 2$عنصراً جامداً مختلفاً، غير مبتذل، وفق ما يأتي:

أ) إذا كان $\left[\frac{k}{2}\right]$ فردياً، حيث $\left[\frac{k}{2}\right]$ ترمز إلى القسم الصحيح لـ $\frac{k}{2}$ ، فإنه:

-١- من أجل كل $P_i \equiv \alpha_i (\bmod q_i)$ ، حيث i من $\{1,2,..,k\}$ و $q_i = \frac{n}{P_i}$ ، يوجد عنصر ان جامدان، غير مبتذلين، هما:

$$e_i = \alpha_i^{\varphi(q_i)-1} P_i \quad \text{و} \quad f_i = 1 - e_i$$

بالتالي من أجل جميع قيم α_i، و حيث k عدد القواسم الأولية المختلفة للعدد n، نحصل على $C_k^1 + C_k^{k-1}$ عنصراً جامداً مختلفاً، غير مبتذل،(وحيث ترمز C_k^i إلى توافيق الـ i عنصر مأخوذة من k عنصر).

٢- من أجل كل $P_l \,.P_j \equiv \beta_{lj} (\bmod\ q_{lj})$، حيث عدد β_{lj} هو C_k^2، و لكل $l \neq j$ من $\{1,2,..,k\}$ و $q_{lj} = \dfrac{n}{P_l \,.P_j}$ يوجد عنصر ان جامدان، غير مبتذلين، هما:

$$f_{lj} = 1 - e_{lj} \text{ و } e_{lj} = \beta_{lj}^{\varphi(q_{lj})-1} P_l \,.P_j$$

بالتالي من أجل جميع قيم β_{lj}، و حيث k عدد الأعداد الأولية المختلفة، نحصل على $C_k^2 + C_k^{k-2}$ عنصراً جامداً مختلفاً، غير مبتذل.

٣- وهكذا حتى نصل إلى أن عدد المضاريب $P_{i_1}, P_{i_2}, .., P_{i_m}$ المختلفة يساوي إلى $m = \left[\dfrac{k}{2}\right]$، فيكون من أجل كل $P_{i_1} .P_{i_2} ...P_{i_m} \equiv \gamma_{i_1 i_2 ..i_m} (\bmod\ q_{i_1 i_2 ..i_m})$، حيث عدد $\gamma_{i_1 i_2 ..i_m}$ هو C_k^m و لكل $i_1 \neq i_2 \neq .. \neq i_m$ من $\{1,2,..,k\}$ و $q_{i_1 i_2 ..i_m} = \dfrac{n}{P_{i_1} .P_{i_2} ...P_{i_m}}$ يوجد عنصر ان جامدان، غير مبتذلين، هما:

$$f_{i_1 i_2 ..i_m} = 1 - e_{i_1 i_2 ..i_m} \text{ و } e_{i_1 i_2 ..i_m} = \gamma_{i_1 i_2 ..i_m}^{\varphi(q_{i_1 i_2 ..i_m})-1} P_{i_1} .P_{i_2} ...P_{i_m}$$

بالتالي، من أجل جميع قيم $\gamma_{i_1 i_2 ..i_m}$، و حيث k عدد الأعداد الأولية المختلفة، نحصل على $C_k^m + C_k^{k-m}$ عنصراً جامداً مختلفاً، غير مبتذل.

ب) إذا كان $\left[\dfrac{k}{2}\right]$ زوجياً، فإنه:

١- من أجل كل $P_i \equiv \alpha_i (\bmod\ q_i)$، حيث i من $\{1,2,..,k\}$ و $q_i = \dfrac{n}{P_i}$، يوجد عنصر جامد، غير مبتذل، هو:

$$e_i = \alpha_i^{\varphi(q_i)-1} P_i$$

بالتالي من أجل جميع قيم α_i، و حيث k عدد القواسم الأولية المختلفة للعدد n، نحصل على C_k^1 عنصراً جامداً مختلفاً، غير مبتذل،(وحيث ترمز C_k^i إلى توافيق الـ i عنصر مأخوذة من k عنصر).

-٢- من أجل كل $P_l \, .P_j \equiv \beta_{lj} (\bmod \, q_{lj})$، حيث عدد β_{lj} هو C_k^2، و لكل $l \neq j$ من $\{1,2,..,k\}$ و $q_{lj} = \frac{n}{P_l \, .P_j}$، يوجد عنصر جامد، غير مبتذل، هو:

$$e_{lj} = \beta_{lj}^{\varphi(q_{lj})-1} P_l \, .P_j$$

بالتالي، من أجل جميع قيم β_{lj}، و حيث k عدد الأعداد الأولية المختلفة، نحصل على C_k^2 عنصراً جامداً مختلفاً، غير مبتذل.

-٣- وهكذا حتى نصل إلى أن عدد المضاريب $P_{i_1}, P_{i_2}, ..., P_{i_m}$ المختلفة يساوي إلى $m = k-1$، فيكون من أجل كل $P_{i_1} .P_{i_2} ... P_{i_m} \equiv \gamma_{i_1 i_2 .. i_m} (\bmod \, q_{i_1 i_2 .. i_m})$، حيث عدد $\gamma_{i_1 i_2 .. i_m}$ هو C_k^m و لكل $i_1 \neq i_2 \neq .. \neq i_m$ من $\{1,2,..,k\}$ و $q_{i_1 i_2 .. i_m} = \frac{n}{P_{i_1} .P_{i_2} ... P_{i_m}}$، يوجد عنصر جامد، غير مبتذل، هو:

$$e_{i_1 i_2 .. i_m} = \gamma_{i_1 i_2 .. i_m}^{\varphi(q_{i_1 i_2 .. i_m})-1} P_{i_1} .P_{i_2} ... P_{i_m}$$

بالتالي من أجل جميع قيم $\gamma_{i_1 i_2 .. i_m}$، و حيث k عدد الأعداد الأولية المختلفة، نحصل على C_k^m، حيث $m = k-1$،عنصراً جامداً مختلفاً، غير مبتذل.

البرهان:

أ) لنبرهن أولاً على أن عدد هذه العناصر هو $2^k - 2$، وثانياً على أنها جامدة ومختلفة وغير مبتذلة، وثالثاً على وحدانيتها.

أولاً:

$$C_k^1 + C_k^{k-1} + C_k^2 + C_k^{k-2} + .. C_k^m + C_k^{k-m} = \sum_{i=1}^{k-1} C_k^i$$

وبالاعتماد على ثنائي الحد لنيوتن نجد أن $2^k = 2 + \sum_{i=1}^{k-1} C_k^i$، أي إن:

$$2^k - 2 = \sum_{i=1}^{k-1} C_k^i$$

أي إن عدد هذه العناصر هو $2^k - 2$.

ثانياً :

بما أن:

$$P_i \equiv \alpha_i (\bmod q_i) \;\; ; \;\; \forall i \in \{1,2,..,k\}$$

فإنه بضرب الطرفين بـ $\alpha_i^{\varphi(q_i)-1}$، نجد:

$$\alpha_i^{\varphi(q_i)-1}.P_i \equiv \alpha_i^{\varphi(q_i)} (\bmod q_i)$$

وبملاحظة أن: $\gcd(\alpha_i, q_i) = \gcd(P_i, q_i) = 1$ يكون استناداً إلى مبرهنة أولر $\alpha_i^{\varphi(q_i)} \equiv 1(\bmod q_i)$، وبالتالي:

$\alpha_i^{\varphi(q_i)-1}.P_i \equiv 1(\bmod q_i)$، أي إن $\alpha_i^{\varphi(q_i)-1}.P_i = 1 + q_i s$، حيث $s \in \mathbf{Z}$، وبضرب الطرفين بـ $(\alpha_i^{\varphi(q_i)-1}.P_i)$ نجد:

$(\alpha_i^{\varphi(q_i)-1}.P_i)^2 = (\alpha_i^{\varphi(q_i)-1}.P_i) + P_i.q_i.s'$، حيث $s' = \alpha_i^{\phi(q_i)-1} s \in \mathbf{Z}$، أي إن:

$$(\alpha_i^{\varphi(q_i)-1}.P_i)^2 \equiv (\alpha_i^{\varphi(q_i)-1}.P_i)(\bmod n)$$

وهذا يعني أن $e_i = (\alpha_i^{\varphi(q_i)-1}.P_i)$ هو عنصر جامد، في الحلقة $\mathbf{Z}_n$ (جامد قياس n).

لنبرهن، الآن، على أن هذه العناصر الجامدة، غير مبتذلة.

*- إذا كان $\alpha_i^{\varphi(q_i)-1}.P_i \equiv 0(\bmod n)$، فإن $n \mid (\alpha_i^{\varphi(q_i)-1}.P_i)$، وبالتالي $q_i \mid (\alpha_i^{\varphi(q_i)-1}.P_i)$، أي إن $\alpha_i^{\varphi(q_i)-1}.P_i \equiv 0(\bmod q_i)$، وهذا مرفوض لأن $\alpha_i^{\varphi(q_i)-1}.P_i \equiv 1(\bmod q_i)$.

*- وإذا كان $\alpha_i^{\varphi(q_i)-1}.P_i \equiv 1(\bmod n)$، فإنه بضرب الطرفين بـ q_i نجد $\alpha_i^{\varphi(q_i)-1}.P_i.q_i \equiv q_i (\bmod n)$، وبالتالي $q_i \equiv 0(\bmod n)$، أي إن $n \mid q_i$، وهذا مرفوض لأن $q_i < n$.

أما البرهان على أن $f_i = 1 - e_i$ هو، أيضاً، عنصر جامد، غير مبتذل، في الحلقة $\mathbf{Z}_n$ فهو واضح.

ولنبرهن، الآن، على أن هذه العناصر هي عناصر مختلفة مثنى مثنى.

لنأخذ i_1, i_2 عددين مختلفين من $\{1,2,..,k\}$ ولنبرهن على أن:

$\alpha_{i_1}^{\varphi(q_{i_1})-1}.P_{i_1}, \alpha_{i_2}^{\varphi(q_{i_2})-1}.P_{i_2}$ مختلفان قياس n.

لنفرض، جدلاً، أن:

$$(\alpha_{i_2}^{\varphi(q_{i_2})-1}.P_{i_2}) \equiv (\alpha_{i_1}^{\varphi(q_{i_1})-1}.P_{i_1})(\bmod n)$$

فيكون:

$$n \mid [(\alpha_{i_2}^{\varphi(q_{i_2})-1}.P_{i_2}) - (\alpha_{i_1}^{\varphi(q_{i_1})-1}.P_{i_1})]$$

وبما أن $q_{i_1} \mid n = P_{i_1}.q_{i_1}$، فإنه بالإعتماد على المبرهنة (١-١-٣٥)، نجد:

$$(\alpha_{i_2}{}^{\varphi(q_{i_2})-1}.P_{i_2}) \equiv (\alpha_{i_1}{}^{\varphi(q_{i_1})-1}.P_{i_1})(\bmod q_{i_1})$$

ولدينا حسب مبرهنة أولر $(\alpha_{i_1}{}^{\varphi(q_{i_1})-1}.P_{i_1}) \equiv 1(\bmod q_{i_1})$، بالتالي:

$(\alpha_{i_2}{}^{\varphi(q_{i_2})-1}.P_{i_2}) \equiv 1(\bmod q_{i_1})$، أي أن $q_{i_1} \mid [(\alpha_{i_2}{}^{\varphi(q_{i_2})-1}.P_{i_2})-1]$. (I)

ولدينا، أيضاً، حسب مبرهنة أولر $(\alpha_{i_2}{}^{\varphi(q_{i_2})-1}.P_{i_2}) \equiv 1(\bmod q_{i_2})$، أي أن:

$q_{i_2} \mid [(\alpha_{i_2}{}^{\varphi(q_{i_2})-1}.P_{i_2})-1]$. (II)

من (I) و (II) واعتماداً على المبرهنة (١-١-٣٤)، نجد أن:

$[q_{i_1}, q_{i_2}] \mid [(\alpha_{i_2}{}^{\varphi(q_{i_2})-1}.P_{i_2})-1]$ (III)

ولكن $q_{i_1} = \dfrac{n}{P_{i_1}}$ و $q_{i_2} = \dfrac{n}{P_{i_2}}$، بالتالي $[q_{i_1}, q_{i_2}] = n$، بالعودة إلى (III) نجد:

$$n \mid [(\alpha_{i_2}{}^{\varphi(q_{i_2})-1}.P_{i_2})-1]$$

أي أن $(\alpha_{i_2}{}^{\varphi(q_{i_2})-1}.P_{i_2}) \equiv 1(\bmod n)$، وهذا مرفوض لأن $(\alpha_{i_2}{}^{\varphi(q_{i_2})-1}.P_{i_2})$ جامد غير مبتذل في الحلقة $\mathbf{Z}_n$.

بالمثل نبرهن على أن باقي العناصر هي، أيضاً، عناصر جامدة مختلفة وغير مبتذلة، في الحلقة $\mathbf{Z}_n$.

ثالثاً:

لنفرض أن M هي مجموعة جميع العناصر الجامدة السابقة، أي إن:

$$M = \{e_i, f_i; i \in \{1,2,..,k\}\} \cup \{e_{lj}, f_{lj}; l \neq j \notin \{1,2,..,k\}\} \cup ..$$
$$\cup \{e_{i_1 i_2 .. i_m}, f_{i_1 i_2 .. i_m}; i_1 \neq i_2 \neq .. \neq i_m \in \{1,2,..,k\}\}$$

وليكن x عنصراً جامداً ما، غير مبتذل، في الحلقة $\mathbf{Z}_n$ عندئذٍ $x^2 \equiv x(\bmod n)$ أي $n \mid x(x-1)$ بالتالي، بالاعتماد على أن $\gcd(x, x-1) = 1$، نجد أنه يوجد i من $\{1,2,..,k\}$ بحيث $P_i \mid x$، بالتالي $q_i = \dfrac{n}{P_i} \mid (x-1)$ أو $P_i \mid (x-1)$، بالتالي $q_i \mid x$.

* فإذا كان $P_i \mid x$، فإنه من جهة أولى يكون $x = P_i.s$ (1)، حيث $s \in \mathbf{Z}$، ومن جهة ثانية يكون $q_i \mid (x-1)$، أي $x \equiv 1(\bmod q_i)$ (2)، وبما أنه من أجل أي i من $\{1,2,..,k\}$ يكون $P_i \equiv \alpha_i (\bmod q_i)$، فإنه بالعودة إلى (1) والتعويض في (2)، نجد:

$P_i.s \equiv 1(\bmod q_i)$، بالتالي $P_i.s = 1 + q_i.s'$، حيث $s' \in \mathbf{Z}$.

وبضرب الطرفين بـ $\alpha_i{}^{\varphi(q_i)-1}$ نجد:

$$\alpha_i{}^{\varphi(q_i)-1}.P_i.s = \alpha_i{}^{\varphi(q_i)-1} + \alpha_i{}^{\varphi(q_i)-1}.q_i.s'$$

وبما أن: $\alpha_i^{\varphi(q_i)-1}.P_i \equiv 1(\bmod q_i)$ ، فإن: $s = \alpha_i^{\varphi(q_i)-1} + q_i.s''$ ، حيث $s'' \in \mathbf{Z}$.

وبضرب الطرفين بـ P_i نجد:

$$P_i.s = \alpha_i^{\varphi(q_i)-1}.P_i + n.s''$$

أي إن $x = \alpha_i^{\varphi(q_i)-1}.P_i + n.s''$ ، بمعنى أن $x \equiv \alpha_i^{\varphi(q_i)-1}.P_i(\bmod n)$ ،

أي $x \equiv e_i(\bmod n)$ ، وبالتالي $x \in M$.

* أما إذا كان $q_i \mid x$ ، فإنه من جهة أولى يكون $x \equiv 0(\bmod q_i)$ (1)، ومن جهة ثانية يكون $P_i \mid (x-1)$ ، أي (2) $x = 1 + P_i.s$ ، حيث $s \in \mathbf{Z}$، وبما أنه من أجل أي i من $\{1,2,..,k\}$ يكون $P_i \equiv \alpha_i(\bmod q_i)$ ، فإنه بالعودة إلى (2) والتعويض في (1)، نجد:

$P_i.s \equiv -1(\bmod q_i)$ ، بالتالي $P_i.s = -1 + q_i.s'$ ، حيث $s' \in \mathbf{Z}$، وبضرب الطرفين بـ $\alpha_i^{\varphi(q_i)-1}$ نجد:

$$\alpha_i^{\varphi(q_i)-1}.P_i.s = -\alpha_i^{\varphi(q_i)-1} + \alpha_i^{\varphi(q_i)-1}.q_i.s'$$

وبما أن: $\alpha_i^{\varphi(q_i)-1}.P_i \equiv 1(\bmod q_i)$ ، فإن: $s = -\alpha_i^{\varphi(q_i)-1} + q_i.s''$ ، حيث $s'' \in \mathbf{Z}$.

وبضرب الطرفين بـ P_i نجد:

$$P_i.s = -\alpha_i^{\varphi(q_i)-1}.P_i + n.s''$$

أي إن:

$$x - 1 = -\alpha_i^{\varphi(q_i)-1}.P_i + n.s''$$

بمعنى أن $x \equiv [1 - \alpha_i^{\varphi(q_i)-1}.P_i](\bmod n)$ ، أي $x \equiv f_i(\bmod n)$ ، وبالتالي $x \in M$.

- بالمثل نبرهن، بالاعتماد على $n \mid x(x-1)$ و $\gcd(x, x-1) = 1$ ، أنه يوجد l, j من $\{1,2,..,k\}$ و $l \neq j$ ، بحيث $P_l.P_j \mid x$ ، وبالتالي $q_{lj} = \dfrac{n}{P_l.P_j} \mid (x-1)$ ،

أو $P_l.P_j \mid (x-1)$ وبالتالي $q_{lj} \mid x$.

وسنجد عندها أيضاً أن $x \in M$.

- وهكذا حتى نصل إلى حالة وجود $i_1, i_2, .., i_m$ من $\{1,2,..,k\}$، جميعها مختلفة و $m = \left[\dfrac{k}{2}\right]$ ، بحيث $P_{i_1}.P_{i_2}...P_{i_m} \mid x$ ، وبالتالي $q_{i_1 i_2 .. i_m} = \dfrac{n}{P_{i_1}.P_{i_2}...P_{i_m}} \mid (x-1)$ ،

أو $P_{i_1}.P_{i_2}...P_{i_m} \mid (x-1)$ ، وبالتالي $q_{i_1 i_2 .. i_m} \mid x$.

وسنجد عندها أيضاً أن $x \in M$.

وهو المطلوب.

ب) لنبرهن أولاً على أن عدد هذه العناصر هو $2^k - 2$ وثانياً على أنها جامدة ومختلفة وغير مبتذلة وثالثاً على وحدانيتها.

أولاً:

$$\sum_{i=1}^{k-1} C_k^i = C_k^1 + C_k^2 + .. + C_k^m \quad \text{حيث} \quad m = k-1$$

وبالاعتماد على ثنائي الحد لنيوتن نجد أن $2^k = 2 + \sum_{i=1}^{k-1} C_k^i$، أي إن:

$$2^k - 2 = \sum_{i=1}^{k-1} C_k^i$$

أي إن عدد هذه العناصر هو $2^k - 2$.

ثانياً:

بما أن:

$$P_i \equiv \alpha_i (\bmod q_i) \ ; \ \forall i \in \{1,2,..,k\}$$

فإنه بضرب الطرفين بـ $\alpha_i^{\varphi(q_i)-1}$، نجد:

$$\alpha_i^{\varphi(q_i)-1}.P_i \equiv \alpha_i^{\varphi(q_i)} (\bmod q_i)$$

وبملاحظة أن: $\gcd(\alpha_i, q_i) = \gcd(P_i, q_i) = 1$، يكون استناداً إلى مبرهنة أولر $\alpha_i^{\varphi(q_i)} \equiv 1 (\bmod q_i)$، وبالتالي:

$\alpha_i^{\varphi(q_i)-1}.P_i \equiv 1 (\bmod q_i)$، أي إن $\alpha_i^{\varphi(q_i)-1}.P_i = 1 + q_i s$، حيث $s \in \mathbf{Z}$، وبضرب الطرفين بـ $(\alpha_i^{\varphi(q_i)-1}.P_i)$ نجد:

$(\alpha_i^{\varphi(q_i)-1}.P_i)^2 = (\alpha_i^{\varphi(q_i)-1}.P_i) + P_i.q_i.s'$، حيث $s' = \alpha_i^{\phi(q_i)-1} s \in \mathbf{Z}$، أي إن:

$$(\alpha_i^{\varphi(q_i)-1}.P_i)^2 \equiv (\alpha_i^{\varphi(q_i)-1}.P_i)(\bmod n)$$

وهذا يعني أن $e_i = (\alpha_i^{\varphi(q_i)-1}.P_i)$ هو عنصر جامد، في الحلقة $\mathbf{Z}_n$ (جامد قياس n).

لنبرهن، الآن، على أن هذه العناصر الجامدة، غير مبتذلة.

*- إذا كان $\alpha_i^{\varphi(q_i)-1}.P_i \equiv 0 (\bmod n)$، فإن $n \mid (\alpha_i^{\varphi(q_i)-1}.P_i)$، وبالتالي $q_i \mid (\alpha_i^{\varphi(q_i)-1}.P_i)$، أي إن $\alpha_i^{\varphi(q_i)-1}.P_i \equiv 0 (\bmod q_i)$، وهذا مرفوض لأن $\alpha_i^{\varphi(q_i)-1}.P_i \equiv 1 (\bmod q_i)$.

*- وإذا كان $\alpha_i^{\varphi(q_i)-1}.P_i \equiv 1 (\bmod n)$، فإنه بضرب الطرفين بـ q_i نجد $\alpha_i^{\varphi(q_i)-1}.P_i.q_i \equiv q_i (\bmod n)$، وبالتالي $q_i \equiv 0 (\bmod n)$، أي إن $n \mid q_i$، وهذا مرفوض لأن $q_i < n$.

لنبرهن، الآن، على أن هذه العناصر هي عناصر مختلفة مثنى مثنى.

لنأخذ i_1, i_2 عددين مختلفين من $\{1,2,..,k\}$ ولنبرهن على أن:

$\alpha_{i_1}^{\varphi(q_{i_1})-1}.P_{i_1}, \alpha_{i_2}^{\varphi(q_{i_2})-1}.P_{i_2}$ مختلفان قياس n.

لنفرض، جدلاً، أن:

$$(\alpha_{i_2}^{\varphi(q_{i_2})-1}.P_{i_2}) \equiv (\alpha_{i_1}^{\varphi(q_{i_1})-1}.P_{i_1})(\text{mod} n)$$

فيكون:

$$n \mid [(\alpha_{i_2}^{\varphi(q_{i_2})-1}.P_{i_2}) - (\alpha_{i_1}^{\varphi(q_{i_1})-1}.P_{i_1})]$$

وبما أن $q_{i_1} \mid n = P_{i_1}.q_{i_1}$، فإنه بالإعتماد على المبرهنة (١-١-٣٥)، نجد:

$$(\alpha_{i_2}^{\varphi(q_{i_2})-1}.P_{i_2}) \equiv (\alpha_{i_1}^{\varphi(q_{i_1})-1}.P_{i_1})(\text{mod} q_{i_1})$$

ولدينا حسب مبرهنة أولر $(\alpha_{i_1}^{\varphi(q_{i_1})-1}.P_{i_1}) \equiv 1(\text{mod} q_{i_1})$، بالتالي:

$(\alpha_{i_2}^{\varphi(q_{i_2})-1}.P_{i_2}) \equiv 1 \text{mod} q_{i_1})$، أي أن $q_{i_1} \mid [(\alpha_{i_2}^{\varphi(q_{i_2})-1}.P_{i_2})-1]$. (I)

ولدينا، أيضاً، حسب مبرهنة أولر $(\alpha_{i_2}^{\varphi(q_{i_2})-1}.P_{i_2}) \equiv 1(\text{mod} q_{i_2})$، أي أن:

$q_{i_2} \mid [(\alpha_{i_2}^{\varphi(q_{i_2})-1}.P_{i_2})-1]$. (II)

من (I) و (II) واعتماداً على المبرهنة (١-١-٣٤)، نجد أن:

$[q_{i_1}, q_{i_2}] \mid [(\alpha_{i_2}^{\varphi(q_{i_2})-1}.P_{i_2})-1]$ (III)

ولكن $q_{i_1} = \dfrac{n}{P_{i_1}}$ و $q_{i_2} = \dfrac{n}{P_{i_2}}$، بالتالي $[q_{i_1}, q_{i_2}] = n$، بالعودة إلى (III) نجد:

$$n \mid [(\alpha_{i_2}^{\varphi(q_{i_2})-1}.P_{i_2})-1]$$

أي أن $(\alpha_{i_2}^{\varphi(q_{i_2})-1}.P_{i_2}) \equiv 1(\text{mod} n)$، وهذا مرفوض لأن $(\alpha_{i_2}^{\varphi(q_{i_2})-1}.P_{i_2})$ جامد، غير مبتذل، في الحلقة $\mathbf{Z}_n$.

بالمثل نبرهن على أن باقي العناصر هي، أيضاً، عناصر جامدة مختلفة وغير مبتذلة، في الحلقة $\mathbf{Z}_n$.

ثالثاً:

لنفرض أن M هي مجموعة جميع العناصر الجامدة السابقة، أي إن:

$$M = \{e_i ; i \in \{1,2,..,k\}\} \cup \{e_{lj} ; l \neq j \notin \{1,2,..,k\}\} \cup ..$$
$$\cup \{e_{i_1 i_2 .. i_m} ; i_1 \neq i_2 \neq .. \neq i_m \in \{1,2,..,k\}\}$$

وليكن x عنصراً جامداً ما، غير مبتذل، في الحلقة $\mathbf{Z}_n$ عندئذٍ $x^2 \equiv x(\text{mod}\, n)$ أي $n \mid x(x-1)$ بالتالي، بالاعتماد على أن $\gcd(x, x-1) = 1$، نجد أنه يوجد i من $\{1,2,..,k\}$ بحيث $P_i \mid x$، بالتالي $q_i = \dfrac{n}{P_i} \mid (x-1)$ أو $P_i \mid (x-1)$، بالتالي $q_i \mid x$.

* فإذا كان $P_i \mid x$ ، فإنه من جهة أولى يكون $x = P_i.s$ (1)، حيث $s \in \mathbf{Z}$، ومن جهة ثانية يكون $q_i \mid (x-1)$ أي $x \equiv 1(\bmod q_i)$ (2) .

وبما أنه من أجل أي i من $\{1,2,..,k\}$ يكون $P_i \equiv \alpha_i (\bmod q_i)$ ، فإنه بالعودة إلى (1) والتعويض في (2)، نجد:

$P_i.s \equiv 1(\bmod q_i)$ ، بالتالي $P_i.s = 1 + q_i.s'$ ، حيث $s' \in \mathbf{Z}$.

وبضرب الطرفين بـ $\alpha_i^{\varphi(q_i)-1}$ نجد:

$$\alpha_i^{\varphi(q_i)-1}.P_i.s = \alpha_i^{\varphi(q_i)-1} + \alpha_i^{\varphi(q_i)-1}.q_i.s'$$

وبما أن: $\alpha_i^{\varphi(q_i)-1}.P_i \equiv 1(\bmod q_i)$ ، فإن: $s = \alpha_i^{\varphi(q_i)-1} + q_i.s''$ ، حيث $s'' \in \mathbf{Z}$.

وبضرب الطرفين بـ P_i نجد:

$$P_i.s = \alpha_i^{\varphi(q_i)-1}.P_i + n.s''$$

أي إن $x = \alpha_i^{\varphi(q_i)-1}.P_i + n.s''$ ، بمعنى أن $x \equiv \alpha_i^{\varphi(q_i)-1}.P_i(\bmod n)$ ، أي $x \equiv e_i (\bmod n)$ ، وبالتالي $x \in M$.

* أما إذا كان $q_i \mid x$ ، فإنه من جهة أولى يكون $x \equiv 0(\bmod q_i)$ (1)، ومن جهة ثانية يكون $P_i \mid (x-1)$ أي $x = 1 + P_i.s$ (2)، حيث $s \in \mathbf{Z}$.

وبما أنه من أجل أي i من $\{1,2,..,k\}$، يكون $P_i \equiv \alpha_i (\bmod q_i)$ ، فإنه بالعودة إلى (2) والتعويض في (1)، نجد:

$P_i.s \equiv -1(\bmod q_i)$ ، وبالتالي $P_i.s = -1 + q_i.s'$ ، حيث $s' \in \mathbf{Z}$.

وبضرب الطرفين بـ $\alpha_i^{\varphi(q_i)-1}$ نجد:

$$\alpha_i^{\varphi(q_i)-1}.P_i.s = -\alpha_i^{\varphi(q_i)-1} + \alpha_i^{\varphi(q_i)-1}.q_i.s'$$

وبما أن: $\alpha_i^{\varphi(q_i)-1}.P_i \equiv 1(\bmod q_i)$ ، فإن: $s = -\alpha_i^{\varphi(q_i)-1} + q_i.s''$ ، حيث $s'' \in \mathbf{Z}$.

وبضرب الطرفين بـ P_i نجد:

$$P_i.s = -\alpha_i^{\varphi(q_i)-1}.P_i + n.s''$$

أي إن:

$$x - 1 = -\alpha_i^{\varphi(q_i)-1}.P_i + n.s''$$

بمعنى أن $x \equiv [1 - \alpha_i^{\varphi(q_i)-1}.P_i](\bmod n)$ ، أي $x \equiv f_i (\bmod n)$ ، وبالتالي $x \in M$.

– بالمثل نبرهن، بالاعتماد على $n \mid x(x-1)$ و $\gcd(x, x-1) = 1$ ، أنه يوجد l, j من $\{1,2,..,k\}$ و $l \neq j$ ، بحيث $P_l.P_j \mid x$ ، وبالتالي $q_{lj} = \dfrac{n}{P_l.P_j} \mid (x-1)$ ،

أو $P_l.P_j \mid (x-1)$ ، وبالتالي $q_{lj} \mid x$.

وسنجد عندها،أيضاً ، أن $x \in M$.

– وهكذا حتى نصل إلى حالة وجود $i_1, i_2, .., i_m$ من $\{1,2,..,k\}$، جميعها مختلفة و $m = \left[\frac{k}{2}\right]$، بحيث $P_{i_1}.P_{i_2}...P_{i_m} \mid x$، بالتالي $q_{i_1 i_2 ..i_m} = \frac{n}{P_{i_1}.P_{i_2}...P_{i_m}} \mid (x-1)$،

أو $P_{i_1}.P_{i_2}...P_{i_m} \mid (x-1)$، بالتالي $q_{i_1 i_2 ..i_m} \mid x$.

وسنجد عندها،أيضاً ، أن $x \in M$.

وهو المطلوب.

***نتيجة (٢–١–١٦):**

لتكن الحلقة $\mathbf{Z}_n$، بحيث $n = P_1^{i_1}.p_2^{i_2}.....p_k^{i_k}$ و $P_1, P_2, .., P_k$ أعداد أولية مختلفة، عندئذ تحوي الحلقة $\mathbf{Z}_n$، فقط، $2^k - 2$ عنصراً جامداً مختلفاً ، غير مبتذل، وفق ما يآتي:

لنضع $P'_j = P_j^{i_j}$ حيث j من $\{1,2,..,k\}$ عندئذٍ :

أ) إذا كان $\left[\frac{k}{2}\right]$ فردياً ، فإنه:

–١– من أجل كل $P'_j = P_j^{i_j} \equiv \alpha_j (\bmod q_j)$، لكل j من $\{1,2,..,k\}$ و $q_j = \frac{n}{P'_j}$،

يوجد عنصر ان جامدان مختلفان،و غير مبتذلين، هما:

$$f_j = 1 - e_j \quad و \quad e_j = \alpha_j^{\varphi(q_j)-1} P'_j$$

بالتالي من أجل جميع قيم α_j، و حيث k عدد الأعداد الأولية المختلفة، نحصل على $C_k^1 + C_k^{k-1}$عنصراً جامداً مختلفاً ، غير مبتذل.

–٢– من أجل كل $P'_s \, .P'_r \equiv \beta_{sr} (\bmod q_{sr})$، حيث عدد β_{sr} هو C_k^2 ولكل $s \neq r$ من $\{1,2,..,k\}$ و $q_{sr} = \frac{n}{P'_s \, .P'_r}$ يوجد عنصر ان جامدانمختلفان، و غير مبتذلين، هما:

$$f_{sr} = 1 - e_{sr} \quad و \quad e_{sr} = \beta_{sr}^{\varphi(q_{sr})-1} P'_s \, .P'_r \, .$$

بالتالي من أجل جميع قيم β_{sr} ، و حيث k عدد الأعداد الأولية المختلفة، نحصل على $C_k^2 + C_k^{k-2}$عنصراً جامداً مختلفاً ، غير مبتذل.

–٣– وهكذا حتى نصل إلى أن عدد المضاريب $P'_{j_1}, P'_{j_2}, .., P'_{j_m}$ المختلفة يساوي إلى $m = \left[\frac{k}{2}\right]$، فيكون من أجل كل $P'_{j_1} \, .P'_{j_2} ...P'_{j_m} \equiv \gamma_{j_1 j_2 ..j_m} (\bmod q_{j_1 j_2 ..j_m})$،

حيث عدد $\gamma_{j_1 j_2 .. j_m}$ هو C_k^m، و $j_1, j_2, ..., j_m$ من $\{1,2,..,k\}$ و $j_1 \neq j_2 \neq .. \neq j_m$

و $q_{j_1 j_2 .. j_m} = \frac{n}{P'_{j_1} . P'_{j_2} ... P'_{j_m}}$ يوجد عنصر ان جامدان مختلفان، غير مبتذلين، هما:

$$f_{j_1 j_2 .. j_m} = 1 - e_{j_1 j_2 .. j_m} \text{ و } e_{j_1 j_2 .. j_m} = \gamma_{j_1 j_2 .. j_m}^{\varphi(q_{j_1 j_2 .. j_m}) - 1} P'_{j_1} . P'_{j_2} ... P'_{j_m}$$

بالتالي من أجل جميع قيم $\gamma_{j_1 j_2 .. j_m}$، و حيث k عدد الأعداد الأولية المختلفة، نحصل على $C_k^m + C_k^{k-m}$ عنصراً جامداً مختلفاً، غير مبتذل.

أ) إذا كان $\left[\frac{k}{2}\right]$ زوجياً، فإنه:

-١- من أجل كل $P'_j = P_j^{i_j} \equiv \alpha_j (\bmod q_j)$، لكل j من $\{1,2,..,k\}$ و $q_j = \frac{n}{P'_j}$،

يوجد عنصر جامد، غير مبتذل، هو:

$$e_j = \alpha_j^{\varphi(q_j) - 1} P'_j$$

بالتالي من أجل جميع قيم α_j، و حيث k عدد الأعداد الأولية المختلفة، نحصل على C_k^1 عنصراً جامداً مختلفاً، غير مبتذل.

-٢- من أجل كل $P'_s . P'_r \equiv \beta_{sr} (\bmod q_{sr})$، حيث عدد β_{sr} هو C_k^2 ولكل $s \neq r$ من $\{1,2,..,k\}$ و $q_{sr} = \frac{n}{P'_s . P'_r}$، يوجد عنصر جامد، غير مبتذل، هو:

$$e_{sr} = \beta_{sr}^{\varphi(q_{sr}) - 1} P'_s . P'_r$$

بالتالي من أجل جميع قيم β_{sr}، و حيث k عدد الأعداد الأولية المختلفة، نحصل على C_k^2 عنصراً جامداً مختلفاً، غير مبتذل.

-٣- وهكذا حتى نصل إلى أن عدد المضاريب $P'_{j_1}, P'_{j_2}, ..., P'_{j_m}$ المختلفة يساوي إلى $m = k - 1$، فيكون من أجل كل $P'_{j_1} . P'_{j_2} ... P'_{j_m} \equiv \gamma_{j_1 j_2 .. j_m} (\bmod q_{j_1 j_2 .. j_m})$، حيث عدد $\gamma_{j_1 j_2 .. j_m}$ هو C_k^m و $j_1, j_2, ..., j_m$ من $\{1,2,..,k\}$ و $j_1 \neq j_2 \neq .. \neq j_m$

و $q_{j_1 j_2 .. j_m} = \frac{n}{P'_{j_1} . P'_{j_2} ... P'_{j_m}}$، يوجد عنصر جامد، غير مبتذل، هو:

$$e_{j_1 j_2 .. j_m} = \gamma_{j_1 j_2 .. j_m}^{\varphi(q_{j_1 j_2 .. j_m}) - 1} P'_{j_1} . P'_{j_2} ... P'_{j_m}$$

بالتالي من أجل جميع قيم $\gamma_{j_1 j_2 .. j_m}$، و حيث k عدد الأعداد الأولية المختلفة، نحصل على C_k^mعنصراً جامداً مختلفاً، غير مبتذل.

البرهان:

يتم البرهان بنفس أسلوب المبرهنة السابقة.

§.٢ العناصر عديمة القوة في الحلقات $\mathbf{Z}_n$:

تمهيد (٢-٢-١):

لتكن الحلقة $\mathbf{Z}_n$ بحيث n عدد صحيح موجب ما، وليكن x عنصراً عديم القوة في الحلقة $\mathbf{Z}_n$.

بما أن العنصر x عديم القوة، فإنه يوجد عدد صحيح موجب $k \neq 0$ بحيث $x^k \equiv 0(\mathrm{mod}\, n)$، أي $n \mid x^k$، بالتالي:

*- إذا كان $n = P$ عدداً أولياً، فإن $P \mid x^k$، وبما أن P عدد أولي، فإن $P \mid x$، أي إن $x = P.c$، حيث $c \in \mathbf{Z}$، ومنه $x \equiv 0(\mathrm{mod}\, P)$، وهذا يعني أن x عديم القوة مبتذل في الحلقة $\mathbf{Z}_p$.

*- إذا كان $n = p.q$، حيث p, q عددان أوليان، فإن $p.q \mid x^k$، بالتالي $p \mid x^k \,\&\, q \mid x^k$، وبما أن كلاً من p, q عدد أولي، فإن $p \mid x$ و $q \mid x$ و $p.q \mid x$، بالتالي $x = p.q.c$، حيث $c \in \mathbf{Z}$، ومنه $x \equiv 0(\mathrm{mod}\, p.q)$ وهذا يعني أن x عديم القوة مبتذل في الحلقة $\mathbf{Z}_{p.q}$، بالتالي لايوجد سوى الصفر بقوة معدومة في $\mathbf{Z}_{p.q}$.

*- إذا كان $n = P^i$، حيث P عدد أولي و $i > 1$، فإن $P^i \mid x^k$، وبما أن P عدد أولي، فإن $P \mid x$، أي إن $x = P.c$، حيث $c \in \mathbf{Z}$، ومنه $x \equiv P(\mathrm{mod}\, P^i)$ وهذا يعني أن x عديم القوة، غير مبتذل، في الحلقة $\mathbf{Z}_{p^i}$ (قياس $n = P^i$)، بالتالي توجد عناصر عديمة القوة في الحلقة $\mathbf{Z}_{p^i}$ (قياس $n = P^i$) غير مبتذلة.

***تعريف (٢-٢-٢):**

لتكن R حلقة تحوي عناصر عديمة القوة، غير مبتذلة، وليكن x عنصراً عديم القوة غير مبتذل في R، عندئذٍ نقول عن x إنه عنصر عديم القوة أساسي إذا كان هذا العنصر يولد جميع العناصر عديمة القوة الأخرى في الحلقة R.

***مبرهنة (٢-٢-٣):**

لتكن الحلقة $\mathbf{Z}_n$ بحيث n عدد صحيح موجب من الشكل $n = P^i$، حيث P عدد أولي و $i > 1$ عندئذٍ الحلقة $\mathbf{Z}_n$تحوي عنصراً عديم القوة أساسياً واحداً, فقط, هو $x = P$ ودرجة

انعدامه هي $k=i$, ويكون عدد جميع العناصر عديمة القوة، غير المبتذلة، بما في ذلك العنصر عديم القوة الأساسي، مساوياً إلى $\frac{n}{x}-1$ أي $P^{i-1}-1$.

البرهان:

من الواضح، اعتماداً على التمهيد (٢–٢–١)، أن $x=P$ هو عنصر عديم القوة ودرجة انعدامه هي $k=i$ ، لأن $x^i=P^i\equiv 0(\bmod P^i)$ ، ولنبرهن على أن $x=P$ أساسي.

ليكن a عنصراً عديم القوة في الحلقة $\mathbf{Z}_n$ عندئذٍ يوجد عدد صحيح موجب $m>1$ ، بحيث يكون $a^m=0$ أي إن $a^m\equiv 0(\bmod P^i)$ ، وبالتالي $P^i\,|\,a^m$ ، وبما أن $P\,|\,P^i$ ، فإن $P\,|\,a^m$ ، وبما أن P عدد أولي، فإن $P\,|\,a$ ، وبالتالي $a=P.\beta=x.\beta$ ، حيث $\beta\in\mathbf{Z}$ ، وهذا يعني أن a مولد بالعنصر x ، أي إن $a\in(x)$ ، أي إن x هو عنصر عديم القوة أساسي، ويبرهن بسهولة على صحة عدد العناصر عديمة القوة غير المبتذلة.

***مبرهنة (٢–٢–٤):**

لتكن الحلقة $\mathbf{Z}_n$ بحيث n عدد صحيح موجب من الشكل $n=p^i.q^j$ ، حيث $i,j>1$, عندئذٍ الحلقة $\mathbf{Z}_n$تحوي عنصراً عديم القوة أساسياً واحداً, فقط, هو $x=p.q$ ودرجة انعدامه هي $k=\max\{i,j\}$, و يكون عدد جميع العناصر عديمة القوة، غير المبتذلة، بما في ذلك العنصر عديم القوة الأساسي، مساوياً إلى $\frac{n}{x}-1$ أي $p^{i-1}.q^{j-1}-1$.

البرهان:

إن $x=p.q$ هو عنصر عديم القوة ودرجة انعدامه هي $k=\max\{i,j\}$ ، لأن $x^k=p^k.q^k=p^i.p^{k-i}.q^j.q^{k-j}=c.p^i.q^j\equiv 0(\bmod p^i.q^j)$ ، حيث $c=p^{k-i}.q^{k-j}$ ، ولنبرهن على أن $x=p.q$ أساسي.

ليكن a عنصراً عديم القوة في الحلقة $\mathbf{Z}_n$ عندئذٍ يوجد عدد صحيح موجب $m>1$ بحيث يكون $a^m=0$ ، أي إن $a^m\equiv 0(\bmod p^i.q^j)$ ، وبالتالي $p^i.q^j\,|\,a^m$ ، وبما أن $p\,|\,p^i.q^j$ و $q\,|\,p^i.q^j$ ، فإن $p\,|\,a^m$ و $q\,|\,a^m$ ، وبما أن كلاً من p,q عدد أولي، فإن $p\,|\,a$ و $q\,|\,a$ ، وبالتالي $a=p.q.\beta=x.\beta$ ، حيث $\beta\in\mathbf{Z}$ ، وهذا يعني أن a مولد بالعنصر x ، أي إن $a\in(x)$ ، أي إن x هو عنصر عديم القوة أساسي، ويبرهن بسهولة على صحة عدد العناصر عديمة القوة غير المبتذلة.

***مبرهنة (٢-٢-٥):**

لتكن الحلقة $\mathbf{Z}_n$ بحيث n عدد صحيح موجب من الشكل $n = P_1^{i_1}.P_2^{i_2}...P_h^{i_h}$، حيث $i_1, i_2, .., i_h > 1$ عندئذٍ الحلقة $\mathbf{Z}_n$ تحوي عنصراً عديم القوة أساسياً واحداً, فقط, هو $x = P_1.P_2...P_h$ ودرجة انعدامه هي $k = \max\{i_1, i_2, .., i_h\}$, و يكون عدد جميع العناصر عديمة القوة، غير المبتذلة، بما في ذلك العنصر عديم القوة الأساسي، مساوياً إلى $\frac{n}{x} - 1$ أي $P_1^{i_1-1}.P_2^{i_2-1}...P_h^{i_h-1} - 1$.

البرهان:

يتم البرهان بنفس أسلوب المبرهنة السابقة.

§٣. العناصر الجامدة في الحلقات الإقليدية:

تمهيد (٢-٣-١):

بالعودة إلى الملاحظة (١-١-١٨) نجد، اعتماداً على Samuel، أنه إذا كانت $A_1, A_2, ..., A_m$ حلقات إقليدية، فإن $A_1 \times A_2 \times ... \times A_m$ هي، أيضاً، حلقة إقليدية.

تمهيدية (٢-٣-٢):

لتكن R_1, R_2 حلقتين ما، ولتكن $R = R_1 \times R_2$، وليكن $x = (r_1, r_2)$ عنصراً ما من R، عندئذٍ x يكون عنصراً جامداً في الحلقة R إذا، وفقط إذا، كان كل من r_1, r_2 عنصراً جامداً في R_1, R_2 على الترتيب.

البرهان:

لنفرض أن x عنصر جامد في الحلقة R، ولنبرهن على أن كلاً من r_1, r_2 عنصر جامد في R_1, R_2 على الترتيب.

بما أن x عنصر جامد، فإن $x^2 = x$، وبالتالي:

$$x^2 = (r_1, r_2)^2 = (r_1^2, r_2^2) = (r_1, r_2)$$

أي إن:

$$r_1^2 = r_1, r_2^2 = r_2$$

العكس لنفرض، الآن، أن كلاً من r_1, r_2 عنصر جامد في R_1, R_2 على الترتيب، ولنبرهن على أن x عنصر جامد في الحلقة R.

بما أن كلاً من r_1, r_2 عنصر جامد، فإن $r_1^2 = r_1, r_2^2 = r_2$، وبالتالي:

$$x^2 = (r_1, r_2)^2 = (r_1^2, r_2^2) = (r_1, r_2) = x$$

أي إن x عنصر جامد في الحلقة R.

***نتيجة (٢-٣-٣):**

إذا كانت R_1, R_2 حلقتين إقليديتين جوامد كل منهما مبتذلة، وكانت $R = R_1 \times R_2$ ، فإنه بالاعتماد على أن العناصر الجامدة في R_i (حيث $i = 1,2$) هي، فقط، $\{0,1\}$ نجد أن العناصر الجامدة، غير المبتذلة، في الحلقة R الاقليدية هي من الشكل $(0,1)$ أو $(1,0)$.

***مبرهنة (٢-٣-٤):**

لتكن $R_1, R_2,.., R_k$ حلقات ما، ولتكن $R = R_1 \times R_2 \times .. \times R_k$ ، وليكن $x = (r_1, r_2,.., r_k)$ عنصراً ما من R، عندئذ x يكون عنصراً جامداً في الحلقة R إذا، وفقط إذا، كان كل من $r_1, r_2,.., r_k$ عنصراً جامداً في $R_1, R_2,.., R_k$ على الترتيب.

البرهان:

يتم البرهان بذات أسلوب التمهيدية (٢-٣-٢).

***نتيجة (٢-٣-٥):**

إذا كانت $R_1, R_2,.., R_k$ حلقات إقليدية جوامد كل منها مبتذلة، فإنه بالاستناد إلى النتيجة (٢-٣-٣) والمبرهنة (٢-٣-٤) نجد أن العناصر الجامدة، غير المبتذلة، في الحلقة $R = R_1 \times R_2 \times .. \times R_k$ الاقليدية، هي من الشكل $(\alpha_1, \alpha_2,.., \alpha_k)$، حيث α_i ($i = 1,2,.., k$) تنتمي إلى المجموعة $\{1,0\}$ وليست جميعها أصفاراً وليست جميعها أحاداً، ويكون عدد تلك العناصر الجامدة، غير المبتذلة، هو $2^k - 2$ ، وهذا يتطابق مع ما وجدناه سابقاً.

مثال (٢-٣-٥):

لتكن $R = Z[i] \times \Re[x]$ ، حيث $Z[i]$ حلقة صحاح غوص و $\Re[x]$ هي حلقة كثيرات الحدود بمتحول واحد فوق حقل الأعداد الحقيقية $\Re$، من الواضح أن كلاً من $Z[i]$ و $\Re[x]$ هي حلقة إقليدية ولا تحوي أية عناصر جامدة غير مبتذلة، ولكن الحلقة R تحوي، فقط، عنصرين جامدين غير مبتذلين هما $(0,1)$ و $(1,0)$.

الملخص و النتائج:

درسنا في هذه الرسالة نوعين من العناصر الخاصة في بعض الحلقات، إذ إننا درسنا العناصر الجامدة والعناصر عديمة القوة وحاولنا بداية الإجابة عن التساؤلات التالية:

- متى تحوي الحلقة $\mathbf{Z}_n$ عناصر جامدة غير مبتذلة، وما هو شكل هذه العناصر إن وجدت.
- متى تحوي الحلقة $\mathbf{Z}_n$ عناصر عديمة القوة غير مبتذلة، وما هو شكل هذه العناصر إن وجدت.
- متى تحوي الحلقات الإقليدية عناصر جامدة غير مبتذلة، وما هو شكل هذه العناصر إن وجدت.

وكان من أهم النتائج التي تم التوصل إليها:

– تحوي الحلقة $\mathbf{Z}_n$ عناصر جامدة غير مبتذلة إذا، وفقط إذا، كان العدد الصحيح الموجب n غير أولي وعدد قواسم العدد n الأولية المختلفة أكبر من 2، و العدد الصحيح الموجب n هو الذي يحدد شكلها.

– تحوي الحلقة $\mathbf{Z}_n$ عناصر عديمة القوة غير مبتذلة إذا، وفقط إذا، كان العدد الصحيح الموجب n غير أولي وغير بسيط [2]، و العدد الصحيح الموجب n هو الذي يحدد شكلها.

– لتكن الحلقة $\mathbf{Z}_n$، بحيث $n = P_1^{i_1}.p_2^{i_2}.....p_k^{i_k}$ و $P_1, P_2,.., P_k$ أعداد أولية مختلفة، عندئذ تحوي الحلقة $\mathbf{Z}_n$، فقط، $2^k - 2$عنصراً جامداً مختلفاً، غير مبتذل، وفق ما يأتي:
لنضع $P'_j = P_j^{i_j}$ حيث j من $\{1,2,..,k\}$ عندئذٍ :

أ) إذا كان $\left[\frac{k}{2}\right]$ فردياً، فإنه:

-١- من أجل كل $P'_j = P_j^{i_j} \equiv \alpha_j (\bmod q_j)$، لكل j من $\{1,2,..,k\}$ و $q_j = \frac{n}{P'_j}$،

يوجد عنصر ان جامدان مختلفان،و غير مبتذلين، هما:

$$f_j = 1 - e_j \quad و \quad e_j = \alpha_j^{\varphi(q_j)-1} P'_j$$

بالتالي من أجل جميع قيم α_j، و حيث k عدد الأعداد الأولية المختلفة، نحصل على $C_k^1 + C_k^{k-1}$عنصراً جامداً مختلفاً، غير مبتذل.

٢- من أجل كل $P'_s\ .P'_r\ \equiv \beta_{sr}(\bmod q_{sr})$، حيث عدد β_{sr} هو C_k^2 ولكل $s \neq r$ من $\{1,2,..,k\}$ و $q_{sr} = \dfrac{n}{P'_s\ .P'_r}$ يوجد عنصر ان جامدانمختلفان، و غير مبتذلين، هما:

$$e_{sr} = \beta_{sr}^{\varphi(q_{sr})-1} P'_s\ .P'_r \text{ و } f_{sr} = 1 - e_{sr} .$$

بالتالي من أجل جميع قيم β_{sr}، و حيث k عدد الأعداد الأولية المختلفة، نحصل على $C_k^2 + C_k^{k-2}$عنصراً جامداً مختلفاً، غير مبتذل.

٣- وهكذا حتى نصل إلى أن عدد المضاريب $P'_{j_1}, P'_{j_2}, .., P'_{j_m}$ المختلفة يساوي إلى $m = \left[\dfrac{k}{2}\right]$، فيكون من أجل كل $P'_{j_1}\ .P'_{j_2} ...P'_{j_m} \equiv \gamma_{j_1 j_2 .. j_m}(\bmod q_{j_1 j_2 .. j_m})$، حيث عدد $\gamma_{j_1 j_2 .. j_m}$ هو C_k^m، و $j_1, j_2, .., j_m$ من $\{1,2,..,k\}$ و $j_1 \neq j_2 \neq .. \neq j_m$ و $q_{j_1 j_2 .. j_m} = \dfrac{n}{P'_{j_1}\ .P'_{j_2} ...P'_{j_m}}$يوجد عنصر ان جامدان مختلفان، غير مبتذلين، هما:

$$e_{j_1 j_2 .. j_m} = \gamma_{j_1 j_2 .. j_m}^{\varphi(q_{j_1 j_2 .. j_m})-1} P'_{j_1}\ .P'_{j_2} ...P'_{j_m} \text{ و } f_{j_1 j_2 .. j_m} = 1 - e_{j_1 j_2 .. j_m}$$

بالتالي من أجل جميع قيم $\gamma_{j_1 j_2 .. j_m}$، و حيث k عدد الأعداد الأولية المختلفة، نحصل على $C_k^m + C_k^{k-m}$عنصراً جامداً مختلفاً، غير مبتذل.

أ) إذا كان $\left[\dfrac{k}{2}\right]$ زوجياً، فإنه:

١- من أجل كل $P'_j = P_j^{i_j} \equiv \alpha_j(\bmod q_j)$، لكل j من $\{1,2,..,k\}$ و $q_j = \dfrac{n}{P'_j}$،

يوجد عنصر جامد، غير مبتذل، هو:

$$e_j = \alpha_j^{\varphi(q_j)-1} P'_j$$

بالتالي من أجل جميع قيم α_j، و حيث k عدد الأعداد الأولية المختلفة، نحصل على C_k^1 عنصراً جامداً مختلفاً، غير مبتذل.

٢- من أجل كل $P'_s\ .P'_r\ \equiv \beta_{sr}(\bmod q_{sr})$، حيث عدد β_{sr} هو C_k^2 ولكل $s \neq r$ من $\{1,2,..,k\}$ و $q_{sr} = \dfrac{n}{P'_s\ .P'_r}$، يوجد عنصر جامد، غير مبتذل، هو:

$$e_{sr} = \beta_{sr}^{\varphi(q_{sr})-1} P'_s \ .P'_r$$

بالتالي من أجل جميع قيم β_{sr} ، و حيث k عدد الأعداد الأولية المختلفة، نحصل على C_k^2عنصراً جامداً مختلفاً ، غير مبتذل.

-٣- وهكذا حتى نصل إلى أن عدد المضاريب $P'_{j_1}, P'_{j_2}, .., P'_{j_m}$ المختلفة يساوي إلى $m = k - 1$ ، فيكون من أجل كل $P'_{j_1} .P'_{j_2} ...P'_{j_m} \equiv \gamma_{j_1 j_2 .. j_m} (\mod q_{j_1 j_2 .. j_m})$ ، حيث عدد $\gamma_{j_1 j_2 .. j_m}$ هو C_k^m و $j_1, j_2, .., j_m$ من $\{1,2,..,k\}$ و $j_1 \neq j_2 \neq .. \neq j_m$ و $q_{j_1 j_2 .. j_m} = \dfrac{n}{P'_{j_1} .P'_{j_2} ...P'_{j_m}}$، يوجد عنصر جامد، غير مبتذل، هو:

$$e_{j_1 j_2 .. j_m} = \gamma_{j_1 j_2 .. j_m}^{\varphi(q_{j_1 j_2 .. j_m})-1} P'_{j_1} \ .P'_{j_2} ...P'_{j_m}$$

بالتالي من أجل جميع قيم $\gamma_{j_1 j_2 .. j_m}$، و حيث k عدد الأعداد الأولية المختلفة، نحصل على C_k^mعنصراً جامداً مختلفاً ، غير مبتذل.

وعليه فإن عدد جميع العناصر الجامدة السابقة المختلفة، غير المبتذلة، هو:

$$C_k^1 + C_k^{k-1} + C_k^2 + C_k^{k-2} + .. C_k^m + C_k^{k-m} = \sum_{i=1}^{k-1} C_k^i = 2^k - 2$$

- لتكن الحلقة $\mathbf{Z}_n$، بحيث n عدد صحيح موجب من الشكل $n = P_1^{i_1} .P_2^{i_2} ...P_h^{i_h}$ ، حيث $i_1, i_2, .., i_h > 1$ عندئذٍ الحلقة $\mathbf{Z}_n$ تحوي عنصر عديم القوة أساسي واحد, فقط, هو $x = P_1 .P_2 ...P_h$ ودرجة انعدامه هي $k = \max\{i_1, i_2, .., i_h\}$, أما باقي العناصر عديمة القوة، غير المبتذلة، في الحلقة $\mathbf{Z}_n$ فهي مولدة عن العنصر الأساسي، أي من الشكل $x' = \lambda .P_1 .P_2 ...P_h$ حيث $\lambda \in \mathbf{Z}$ ، وبالتالي عدد جميع العناصر عديمة القوة، غير المبتذلة، في الحلقة $\mathbf{Z}_n$ بما في ذلك العنصر عديم القوة الأساسي مساوياً إلى $\dfrac{n}{x} - 1$ أي $(P_1^{i_1 - 1} .P_2^{i_2 - 1} ...P_h^{i_h - 1} - 1)$.

- لتكن الحلقات $R_1, R_2, .., R_k$ ولتكن $R = R_1 \times R_2 \times .. \times R_k$ ، فإذا كان $x = (r_1, r_2, .., r_k)$ عنصراً ما من R ، فإن xيكون عنصراً جامداً في الحلقة R إذا، وفقط إذا، كان كل من $r_1, r_2, .., r_k$ عنصراً جامداً في $R_1, R_2, .., R_k$على الترتيب، وا ِذا كانت الحلقات $R_1, R_2, .., R_k$ اقليدية جوامد كل منها مبتذلة، فإننا نجد أن العناصر الجامدة، غير المبتذلة، في الحلقة $R = R_1 \times R_2 \times .. \times R_k$ الاقليدية، هي من الشكل $(\alpha_1, \alpha_2, .., \alpha_k)$ ،

حيث α_i $(i=1,2,..,k)$ تنتمي إلى المجموعة $\{1,0\}$ وليست جميعها أصفاراً وليست جميعها أحاداً ، ، وبالتالي يكون عددها 2^k-2 ، وهو يتطابق مع ما وجدناه سابقاً .

التوصيات:

نظراً لأهمية العناصر عديمة القوة والعناصر الجامدة، التي سبق وأشرنا إليها، وللدور الكبير الذي تأخذه هذه العناصر في تصنيف الحلقات، وفي تطبيقاتها العلمية المختلفة، فإننا نوصي بما يأتي:

- متابعة ما تم التوصل إليه من نتائج، ومحاولة التعميم في الحلقات الاقليدية، والحلقات الأخرى.

- دراسة طبيعة العناصر عديمة القوة، التي حصلنا عليها، وتحديد بنيتها الجبرية.

-دراسة طبيعة العناصر الجامدة، التي حصلنا عليها، وتحديد بنيتها الجبرية.

References - المراجع

1- **سالم السحله** أحمد عبد العزيز، 2002- **العناصر والمثاليات الجامدة في حلقات أشباه الزمر**، رسالة ماجستير، جامعة آل البيت.

2- **ضبيط** نادر، 2004- **العناصر بقوة معدومة في الحلقات $\mathbf{Z}_n$**، مجلة بحوث جامعة حلب، عدد 43، ص 1-12.

3- **عكور** سامر، 2000- **الجوامد في حلقات الزمر**، رسالة ماجستير، جامعة آل البيت.

[4]- Alkam, O., Abu Osba, E., 2007- **On The Regular Elements in $\mathbf{Z}_n$**, *Turk J Math*, 31 , 1-9.

[5]- Burton, D. M., 2001- **Elementary Number Theory**, McGraw Hill, 5^{th}, 411 pages.

[6]- Cohen, H., 1980- **Advanced Number Theory**, Dover Publications Inc., 1^{st}, New York, 275 pages.

[7]- Coelho, S.P., 1998- **Some Remarks on Central Idempotent in Group Rings**, Publ. Math. Debrecen, Vol. 52, No.1.

[8]- Finch, S., 2006- **Idempotent and Nilpotent Modulo n**, http://arxiv.org/abs/math.NT/0605019v1.

[9]- Hardy, G. H., Wright, E. M., 1975- **An Introduction to The Theory of Numbers**, The Clarendon Press, 4^{th}, Oxford, 421 pages.

[10]- Lam, T. Y., 2001- **A First Course in Noncommutative Rings**, John Wiley and Sons Ltd., 2^{nd}, 385 pages.

[11]- Lambek, J., 1986- **Lectures on Rings and Modules**, George Springer, 3^{rd}, 183 pages.

[12]- Le Vque, W. J., 1977- **Fundamentals of Number Theory**, Addision weseley, California, 28 pages.

[13]- Krempa, J., 1980- **Special Elements in Semigroup Rings**, Bulletin de L'Academie, Polonaise des Sciences, Vol. XXVIII, N0.1-2.

[14]- Samuel, P., 1971- **About Euclidean Ring,** Journal of Algebra, Vol. 19, No. 3.

[15]- Sehgal, S. K., 1978- **Topics in Group Rings**, Marcel Dekker, 1^{st}, New York, 251 pages.

[16]- Stark, H. M., 1984- **An Introduction to Number Theory**, Cambridge, Massachusetts: The MIT Press.

[17]- Zariski, O., Samuel, P., 1975- **Commutative Algebra**, New York (u.a.) Springer, Vol -1, Vol -2, 1958-1960 ed, 329 pages.

[18]- Ahmad, M. K., Dabbit, N., Jaddouh, A. A., 2008- **Studying of Idempotent Elements in Some Rings,** Research Journal of Aleppo University, Vol. 60, 135-151.

المصطلحات العلمية

-A-

Algebra	جبر
Anticommutative	غير تبديلي
Associative	تجميعي

-B-

Bilateral ideal	مثالية ثنائية الجانب

-C-

Class	صف
Central	مركزي
Commutative	تبديلي
- **Group**	زمرة تبديلية
- **Ring**	حلقة تبديلية
Complement	متمم
Contain	يحتوي
Contained in	محتوى فى

-D-

Decomposition	تحليل
Degree	درجة
Definition	تعريف
Divide	يقسم

Division	تقسيم
Divisor	قاسم
- **Of zero**	قاسم للصفر
Domine	منطقة

-E-

Element	عنصر
Euclidean ring	حلقة إقليدية

-F-

Factor	عامل
Factorization	تحليل إلى عوامل

-G-

Generated by	ولد بـِ
Group	زمرة

-I-

Ideal	مثالية
Integer number	عدد صحيح
Integral domain	منطقة تكاملية
Invertible	قابل للقلب

-L-

Left ideal	مثالية يسارية

-M-

Matrix	مصفوفة

Maximal ideal	مثالية أعظمية

-O-

Orthogonal	تعامد

-P-

Prime ideal	مثالية أولية
Principal ideal	مثالية رئيسية
Primitive	ابتدائي
Product	جداء

-Q-

Quotient ring	حلقة القسمة

-R-

Radical	جذر
Right ideal	مثالية يمينية
Ring	حلقة

-S-

Set	مجموعة
Subring	حلقة جزئية
Sum	مجموع

-U-

Unique factorization domain	منطقة تحليل وحيد

ABSTRACT:

In this paper we have determined the idempotent and nilpotent elements in Z_n and other rings, and we have tried to answering the following questions:

- **When has the ring Z_n, for some $n \in N$, idempotent and nilpotent elements?**
- **What is the form of these elements if they are existed?**
- **When have the Euclidean rings idempotent?**



Syrian Arab Republic
Aleppo University
Faculty of Sciences
Math. Department

Nilpotent and Idempotent Elements in Some Rings

Presented by

Abd Al-Moean Jaddouh

Supervision

Prof.	Dr.
Mohamad Khayr Ahmad	Nader Dabbit